Azure Monitoring 101

Hands-on lab step-by-step

Lab

Oct 2018

Min Ae Cho (CSA)

Contents

[Monitoring 101 1](#_Toc527920244)

[hands-on lab 1](#_Toc527920245)

[step-by-step 1](#_Toc527920246)

[목표 1](#_Toc527920247)

[Lab 구성 2](#_Toc527920248)

[요구사항 2](#_Toc527920249)

[Lab 1. Azure Log Analytics 3](#_Toc527920250)

[Step 1: Azure Log Analytics 설치 및 구성 4](#_Toc527920251)

[Step 2: Azure Log Analytics에 리소스 연결하기 (VM Agent가 설치되어 있는 경우) 6](#_Toc527920252)

[Step 2.1: Azure Log Analytics에 리소스 연결하기 (VM Agent가 설치되어 있지 않은 경우) 8](#_Toc527920253)

[Lab 2. Azure 로그 분석(Log Analytics) 사용하기 15](#_Toc527920254)

[Lab 3. Azure 보안 센터(Security Center) 사용하기 24](#_Toc527920255)

Monitoring 101

hands-on lab

step-by-step

## 목표

Azure에서 제공하는 모니터링 솔루션(Log Analytics, OMS)을 사용하여 다양한 환경(온프레미스, 클라우드) 의 리소스들을 효율적으로 한 곳에서 모니터링하고 보안 센터(Security Center)를 이용하여 보안을 중점적으로 모니터링하고 외부의 위협을 감지해 더 안전한 보안 아키텍쳐를 구성할 수 있게 한다.

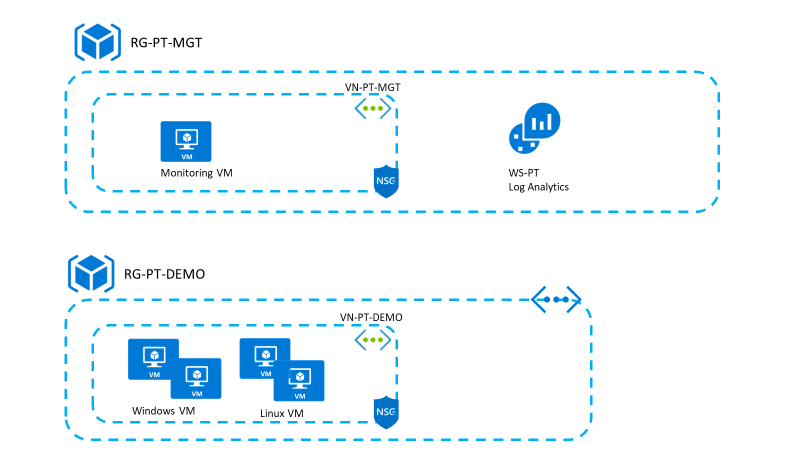
사용하는 Azure 서비스

* Azure 가상머신
* Azure Log Analytics , OMS
* Azure 보안센터 (Security Center)

## Lab 구성

PowerShell을 이용해 배포한 가상 머신들에 Log Analytics를 사용할 수 있게 OMS agent 설치와 구성을 진행한다.

1. 리소스 그룹 : 가상머신 / 네트워크 리소스 관리용도 두개의 리소스 그룹 구성
2. 가상 네트워크 : 두개의 격리된 논리 네트워크 구성
3. 가용성 집합 : 가상머신가용성 집합 구성
4. 네트워크 보안 그룹 : 네트워크 필터링을 위한 보안 그룹 구성
5. Log Analytics :



## 요구사항

* Microsoft Azure subscription
* Local machine
* Lab 1 – 2 실습

## Lab 1. Azure Log Analytics

크게 두가지의 시나리오를 가지고(agent가 설치되어 있지 않은 경우, 설치된 경우) Log Analytics를 사용할 수 있는 방법에 대해 알아보고 실습해봅니다.

Microsoft Azure VM Agent는 Azure 패브릭 컨트롤러와 가상 머신의 상호 작용을 관리하는 안전하고 간단한 프로세스입니다. 가상 머신 Agent는 가상 머신 확장(VM Extension)을 설정하고 실행하는 데 기본적인 역할을 수행합니다. 가상 머신 확장(Virtual Machine Extension)을 사용하면 소프트웨어 설치 및 구성과 같은 가상 머신 배포 후 구성을 설정할 수 있습니다. Azure VM Agent가 없으면 가상 머신 확장을 실행할 수 없습니다. 또한 Azure Backup 또는 Azure Security와 같은 일부 Azure 서비스를 이용할 수 없기 때문에 설치를 권장합니다.

Azure VM Agent는 Azure Marketplace 이미지에서 배포된 모든 Windows VM에 기본적으로 설치됩니다. Azure Portal, PowerShell, 명령줄 인터페이스(Command Line Interface: CLI) 도는 Azure Resource Manager 템플릿에서 Azure Marketplace 이미지를 배포하면 Azure VM Agent도 자동적으로 설치됩니다.

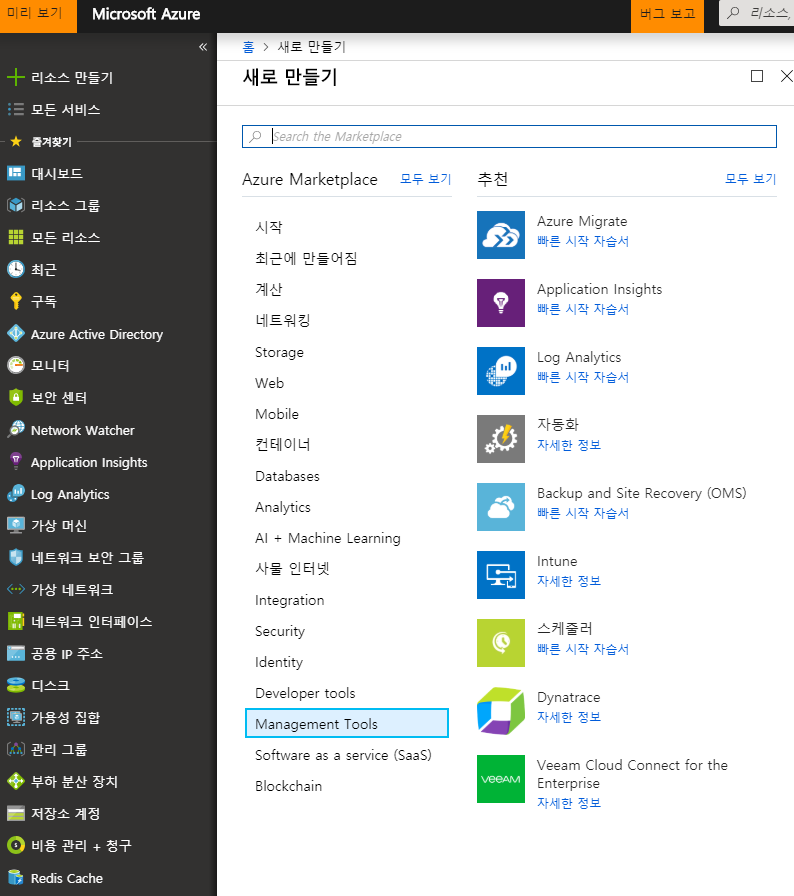
Azure VM Agent의 Windows Guest Agent 패키지는 두 부분으로 나누어있습니다.

* PA(Provision Agent) : VM을 부팅하려면 VM에 PA가 설치되어 있어야합니다.
* WinGA (Windows Guest Agent)

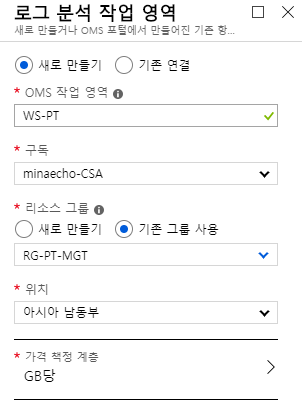
#### Step 1: Azure Log Analytics 설치 및 구성

1. Azure 포탈에서 “리소스 만들기”를 선택 후 “Management Tools”를 선택합니다.

우측에 나오는 서비스 중 Log Analytics를 선택합니다.



1. “새로 만들기” 버튼을 클릭하여 로그 분석 작업 영역을 생성합니다.



**구독 : 사용할 구독 계정 선택**

**리소스 그룹 : 기존 위치 사용 선택 후 RG-PT-MGT 선택**

**위치 : 아시아 남동부**

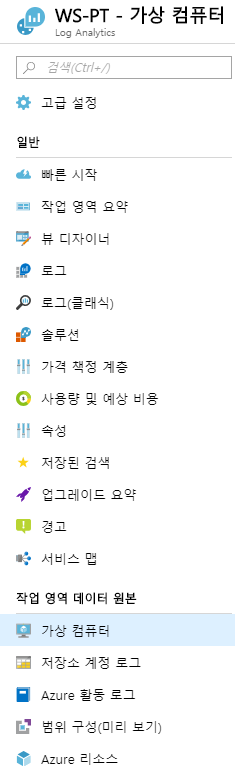
**가격 책정 계층 : GB 당**

1. 아래와 같이 리소스 그룹에 (RG-PT-MGT) 로그 분석(Log Analytics) 리소스가 생성된 것을 확인합니다.

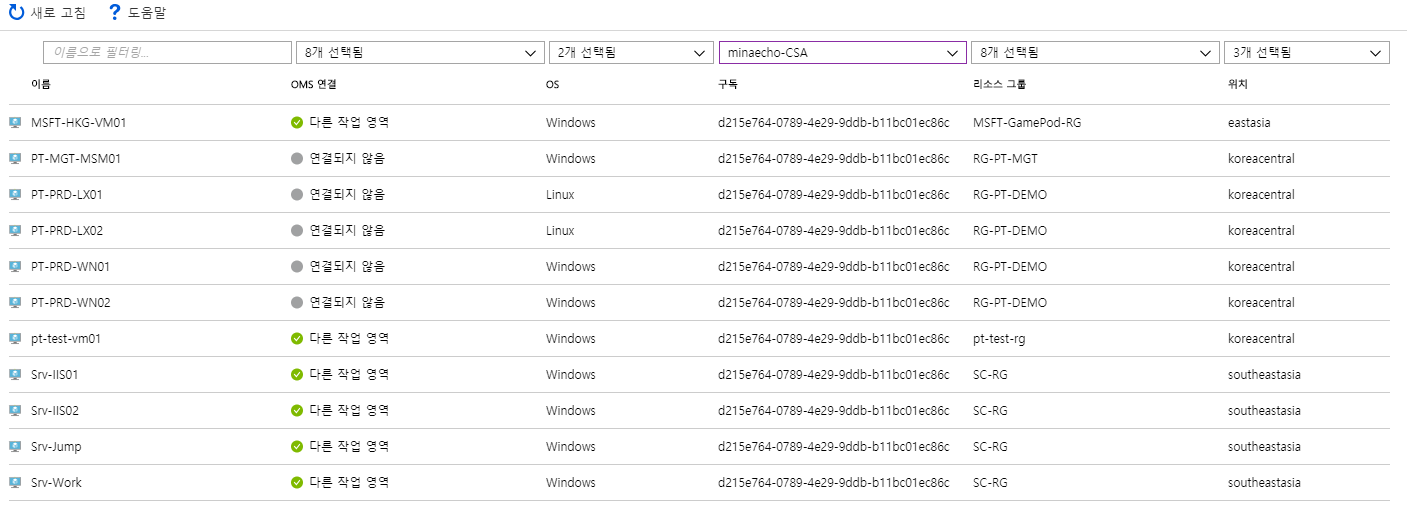


#### Step 2: Azure Log Analytics에 리소스 연결하기 (VM Agent가 설치되어 있는 경우)

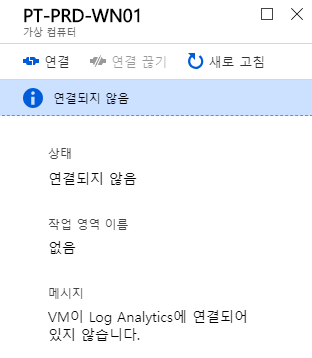
1. Log Analytics 서비스로 이동하여, “작업 영역 데이터 원본” 에서 가상 컴퓨터 버튼을 클릭합니다.



“가상 컴퓨터” 버튼을 누르면 현재 구독에 있는 가상 컴퓨터 목록이 보이며 OMS 연결 여부가 표시됩니다.



1. 연결하려는 가상 머신을 선택합니다. (PT-PRD-WN01) 선택 후 “연결” 버튼을 누릅니다.



실행 중이면 다음과 같은 화면이 나오게 됩니다. 가상머신이 실행 중이지 않거나 Azure VM Agent가 설치되지 않았다면 “오류”가 나타납니다.





가상 머신 Agent가 설치되었다면 Linux 가상 머신도 동일한 방법으로 연결이 가능합니다.

#### Step 2.1: Azure Log Analytics에 리소스 연결하기 (VM Agent가 설치되어 있지 않은 경우)

Azure Marketplace를 통해 가상 머신을 생성하거나 Azure Resource Manager Template, PowerShell, CLI을 이용해서 가상머신을 생성할때 VM Agent 설치를 함께 한다면 VM Agent는 자동으로 설치되어 있습니다.

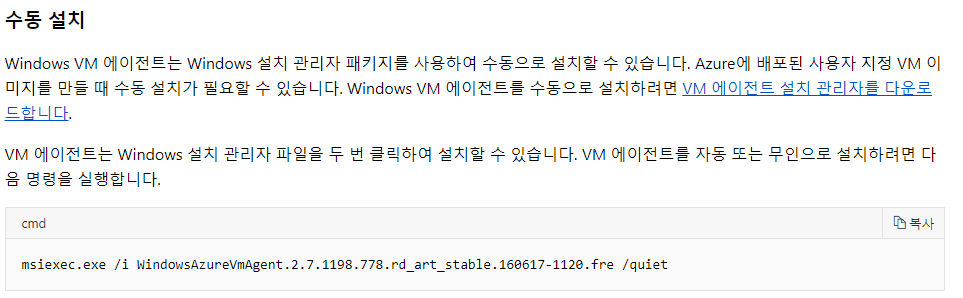
그러나 Custom VHD를 이용해 가상 머신을 생성하거나 VM Agent를 설치하지 않았을 때의 Log Analytics 설정 방법에 대해 알아봅니다. Log Analytics 리소스 생성은 전과 동일하여 생략합니다.

1.VM Agent가 설치되지 않은 가상 컴퓨터에 접속합니다. (ex. 윈도우 : RDP, 리눅스 : SSH 이용)

현재 실습은 윈도우를 기반으로 진행됩니다.

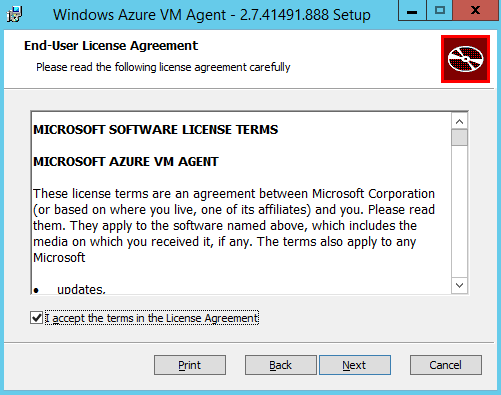
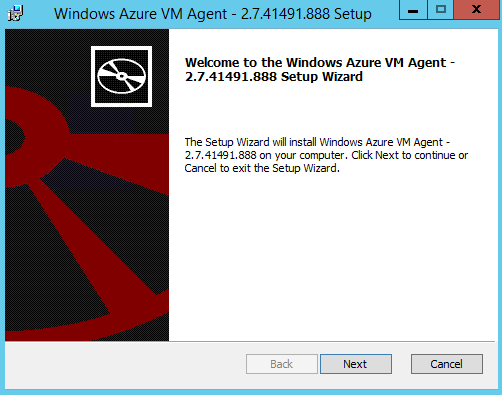
해당 URL 사이트로 이동합니다.

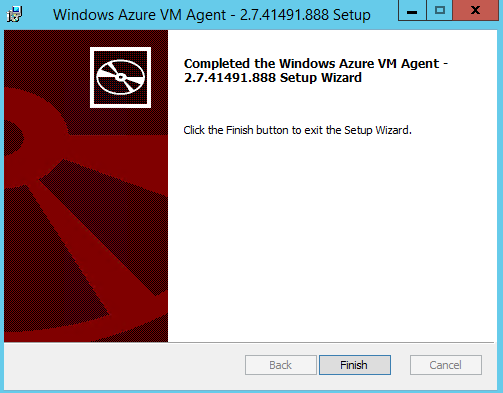
<https://docs.microsoft.com/en-us/azure/virtual-machines/extensions/agent-windows>



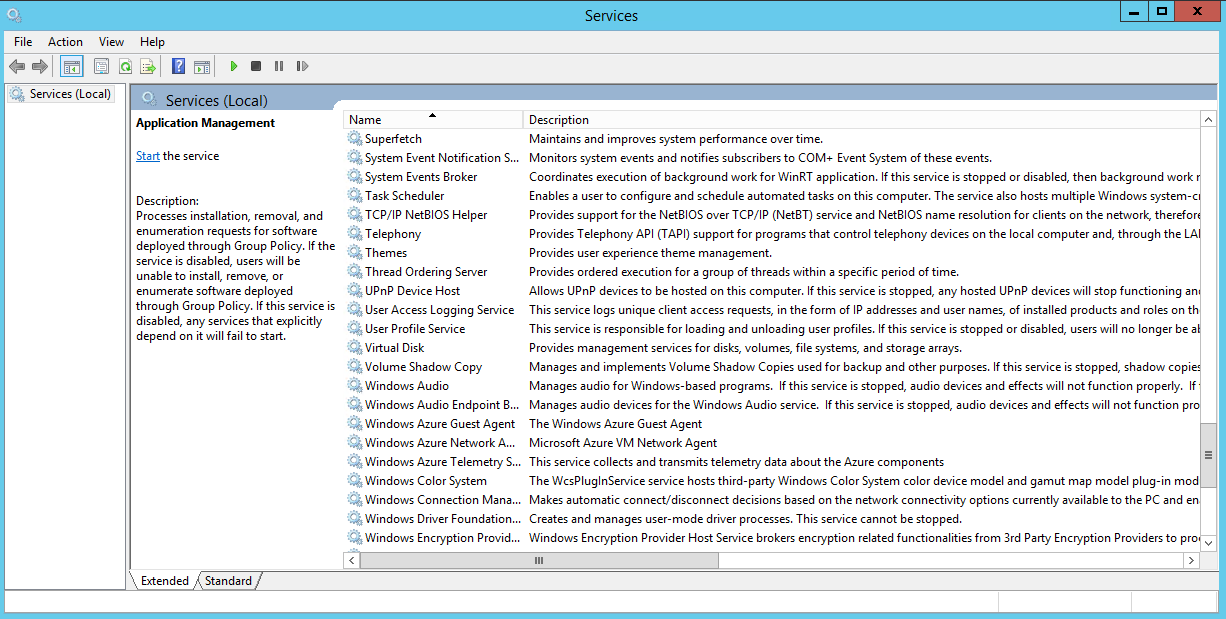
설치에는 두가지 방법이 있으며 url을 통한 다운로드 방법 혹은 CMD 를 이용한 방법이 있습니다.

해당 URL을 클릭하여 설치합니다.



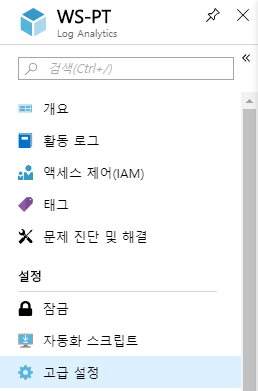


설치가 완료되면 “Services”에서 다음과 같은 Agent를 확인하실 수 있습니다.

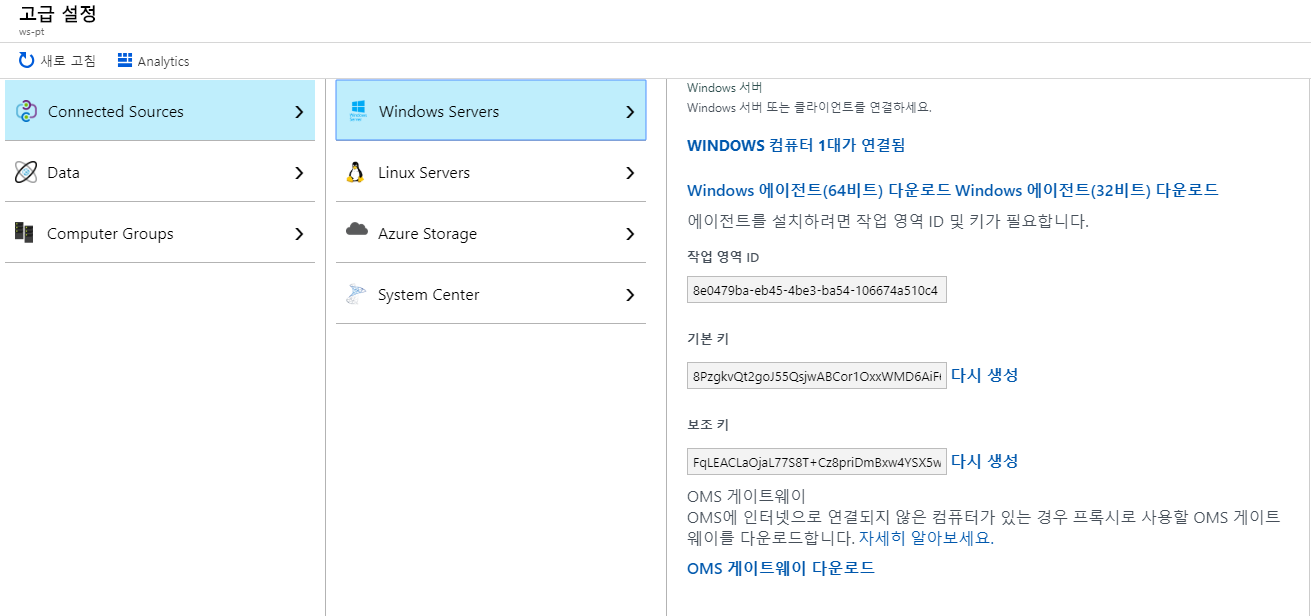


2.Log Analytics는 oms agent를 이용하여 데이터를 수집합니다. Log Analytics는 온프레미스, 클라우드 리소스가 Log Analytics에 연결될 수 있게 agent 및 다운로드 방법을 가이드 하고 있습니다.

Log Analytics 접속 후 “고급 설정” 선택

.

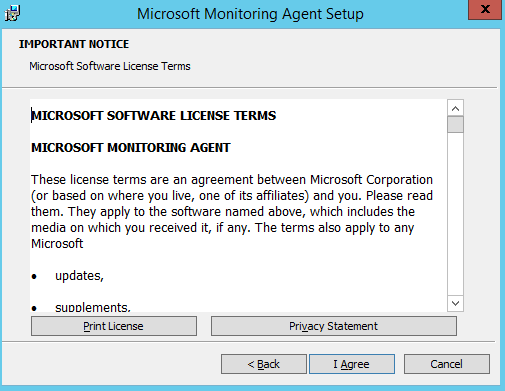
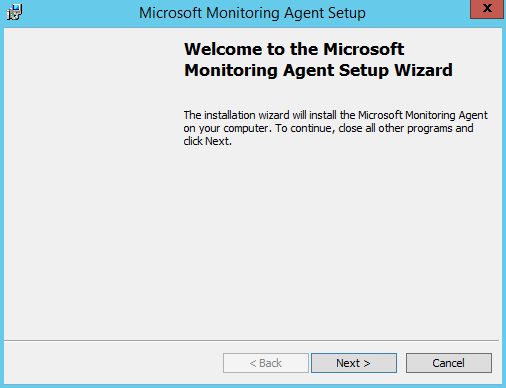
“고급 설정” 선택 후 -> “Connected Sources” -> “Windows Server” 선택

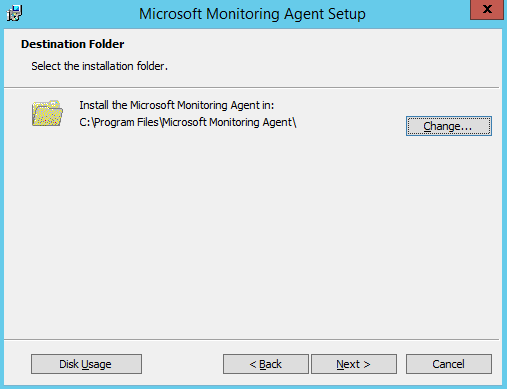


원하는 에이전트 버전을 다운 받습니다.

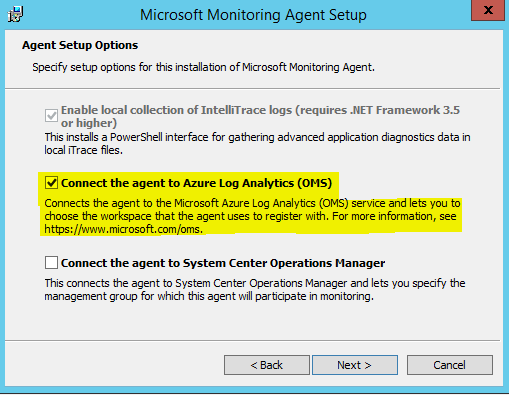


원하는 디렉토리에 넣고 설치를 진행합니다.

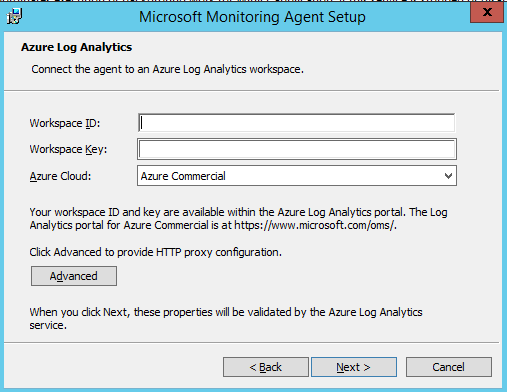




Agent Setup Option이 나왔을 시 “Connect the agent to Azure Log Analytics(OMS)” 을 선택합니다.

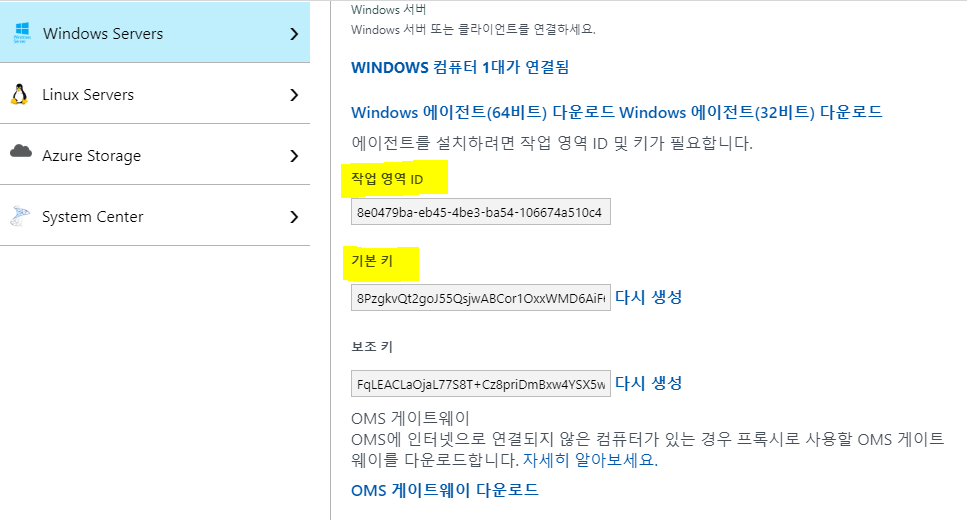


해당 화면이 나왔을때 연결을 위해 Workspace ID, Workspace Key를 입력합니다.



해당 workspace ID와 Workspace Key는

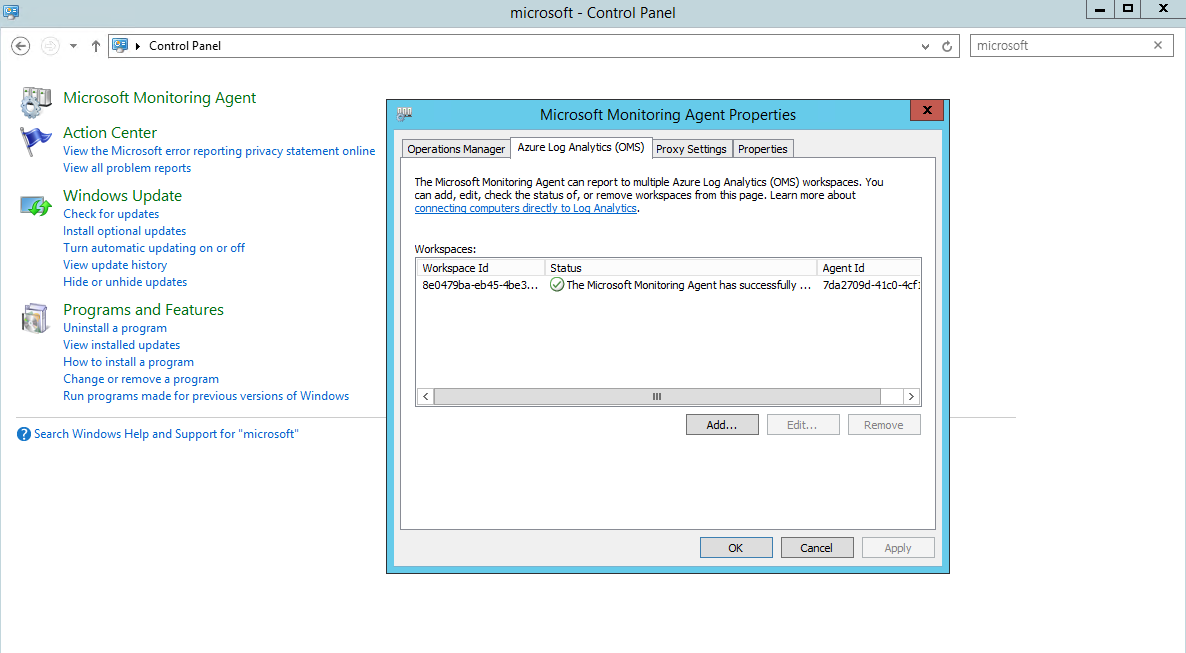
Log Analytics -> 고급 설정 -> Coonected Source 에서 확인합니다.



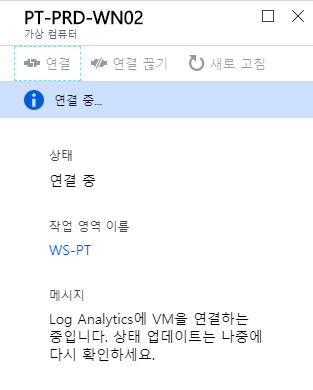
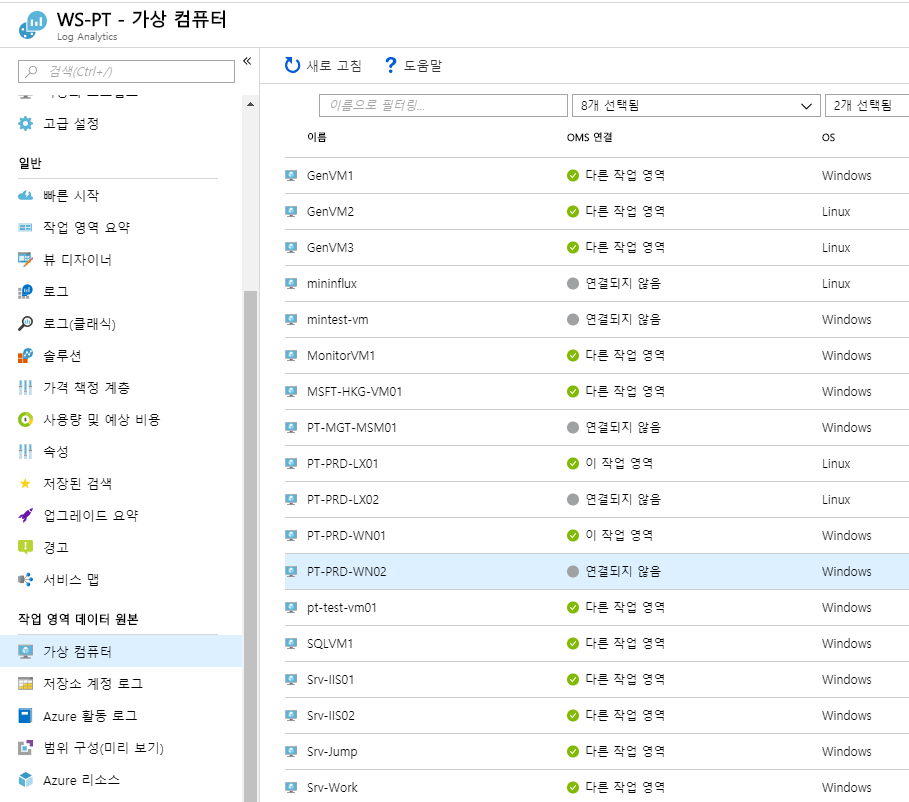
해당 부분을 넣고 설치를 완료합니다.

제어판에 들어가 해당 연결을 확인합니다.

“Control Panel” -> “Microsoft Monitoring Agent” -> Azure Log Analytics(OMS)



확인 후 Azure Portal에 들어가 Log Analytics 에 들어가 해당 가상 머신의 “연결” 버튼을 누릅니다.

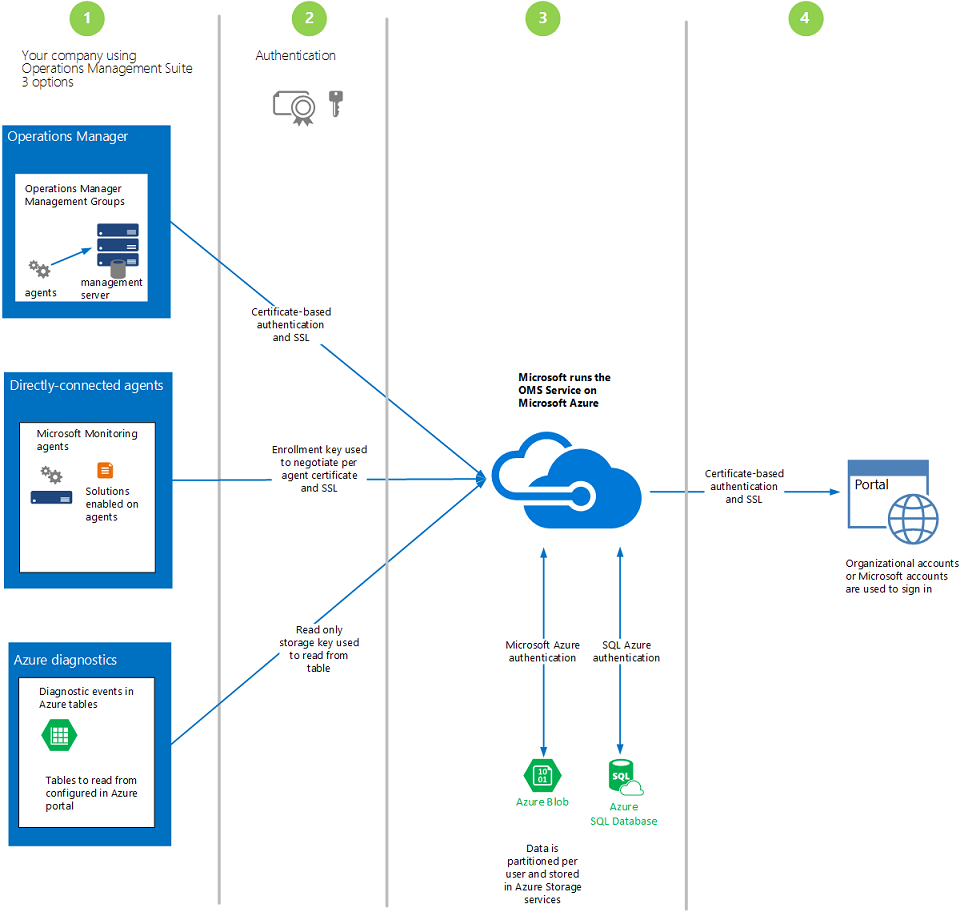


## Lab 2. Azure 로그 분석(Log Analytics) 사용하기

실제 구성을 끝내고 “OMS 포털”을 이용하여 Log Analytics를 사용하는 방법에 대해 간단히 알아봅니다.

“Log Analytics”란 인프라 및 응용프로그램의 로그를 실시간으로 수집, 집계하여 운영을 위한 Insight를 제공하는 서비스입니다. On-Premise 또는 퍼블릭 클라우드(Microsoft Azure, AWS)에 상관없이 사용이 가능합니다.

* 특장점
  + 클라우드 서비스(SaaS) 형태로 제공되기 떄문에 초기 환경 구성 및 서비스 관리의 부담이 없으며 항상 최신 버전의 솔루션을 활용할 수 있습니다.
  + 하나의 서비스에서 통합하여 기존 on-premise 인프라와 클라우드에 구성된 인프라를 한 화면에서 관리할 수 있습니다.
  + 로그 수집을 위한 저장소 관리 및 데이터 관리 노력을 최소화 할 수 있습니다.
  + 수십만 로그를 빠르게 분석할 수 있고 권장 사항과 구체적인 정보를 Microsoft Knowledge Data를 기본으로 제공합니다.
  + Windows와 Linux 모두 OS 수준의 관리가 가능하고 (10초 주기) 성능 수집 및 분석이 가능합니다.



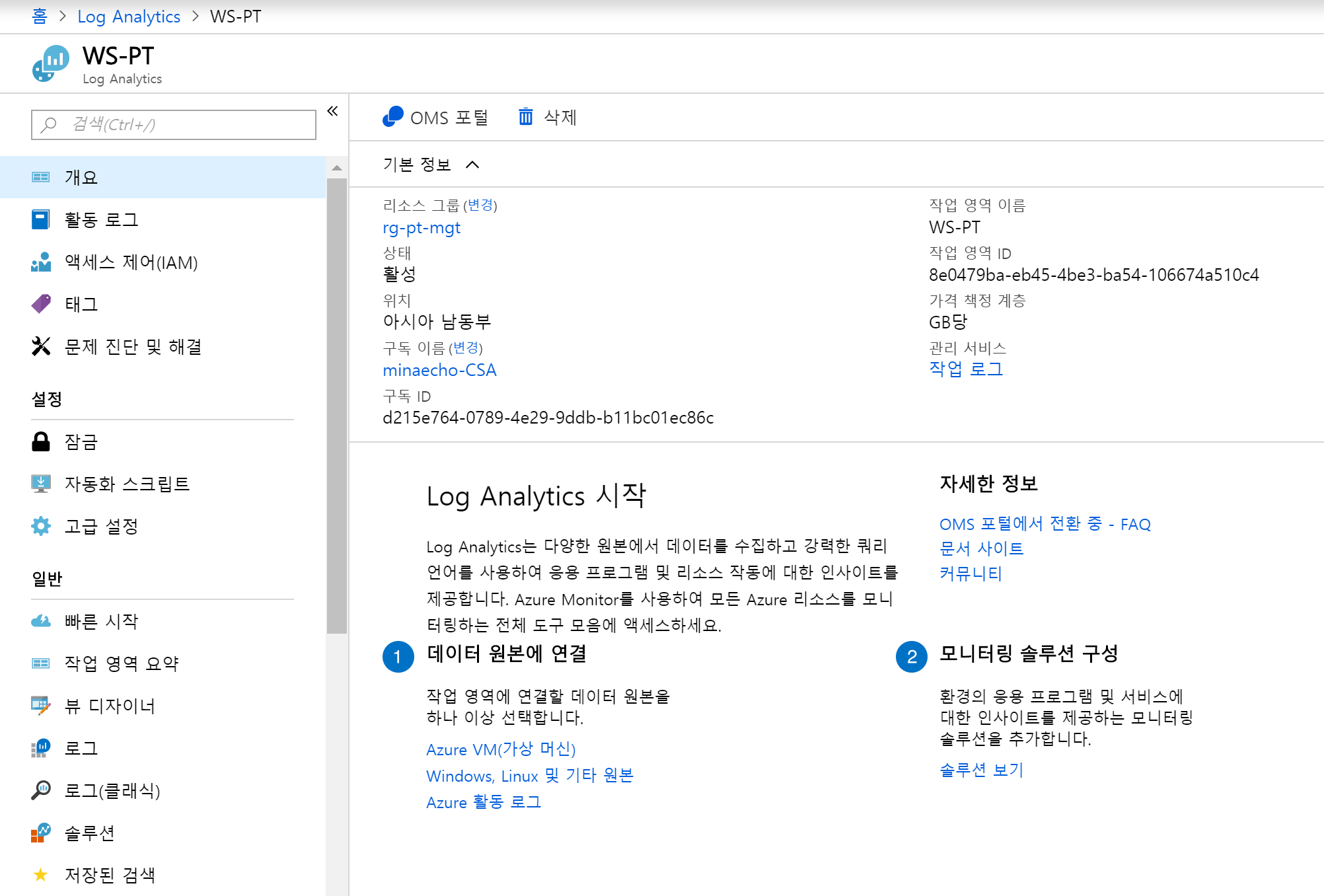
“Log Analytics” 는 솔루션 갤러리 기반으로 서비스를 제공합니다.

크게 4가지 솔루션으로 나뉘어져있습니다 (Insight & Analytics, Automation & Control, Security & Compliance, Protection & Recovery)

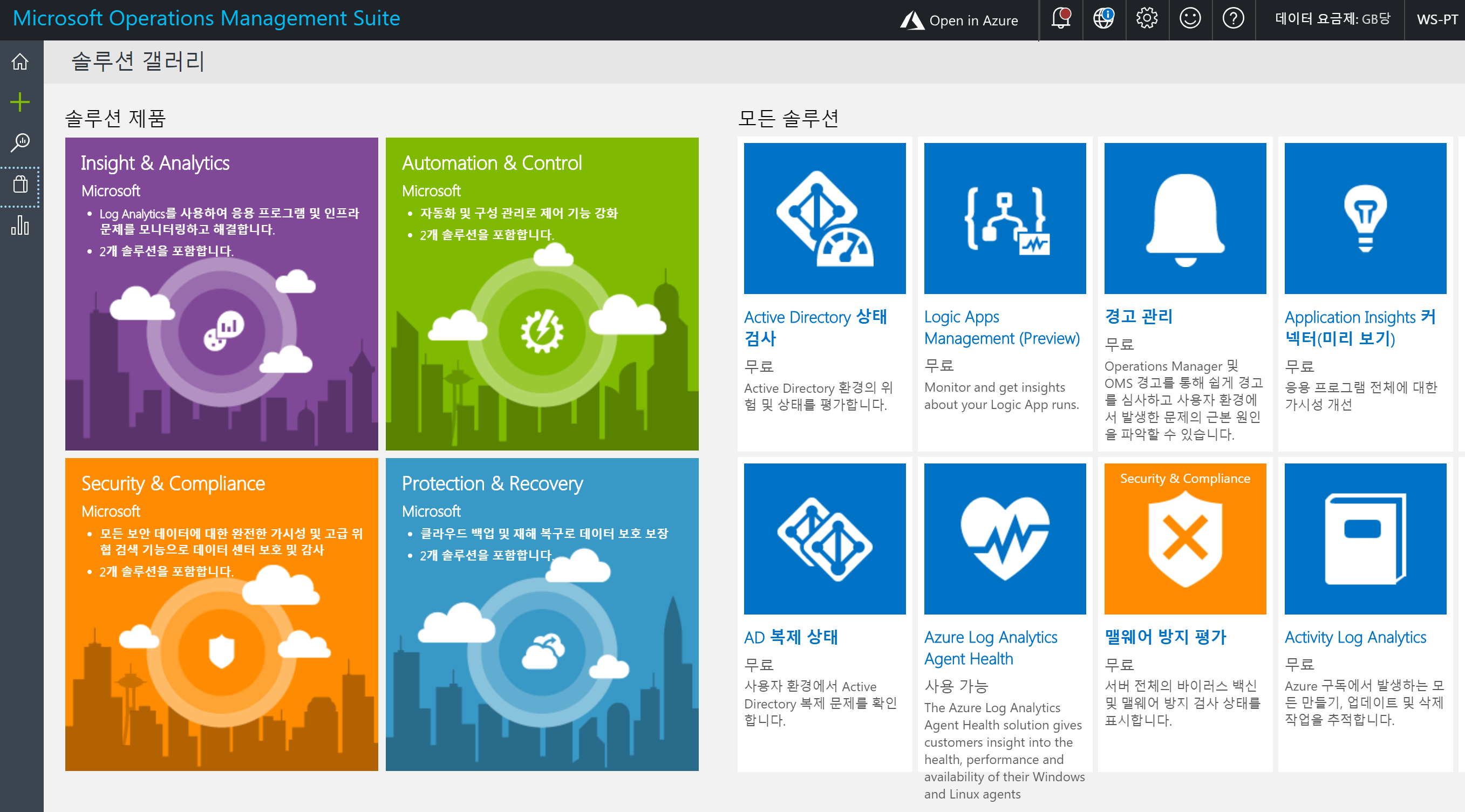


1. Azure Portal 에 접속하여 “Log Analytics” 선택 후

Log analytics -> OMS 포털 선택

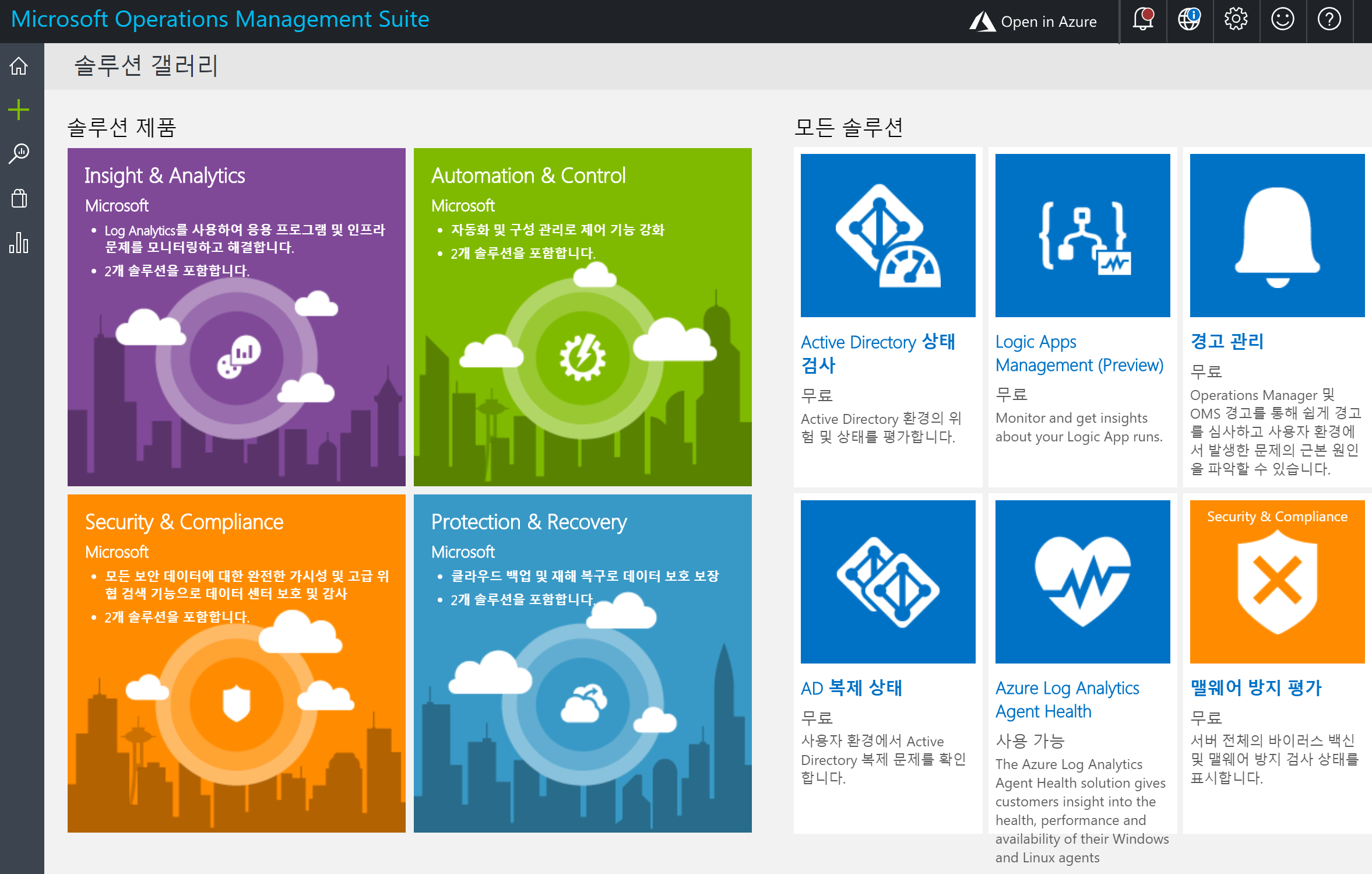


1. OMS 포탈 화면 -> “솔루션 갤러리” 선택



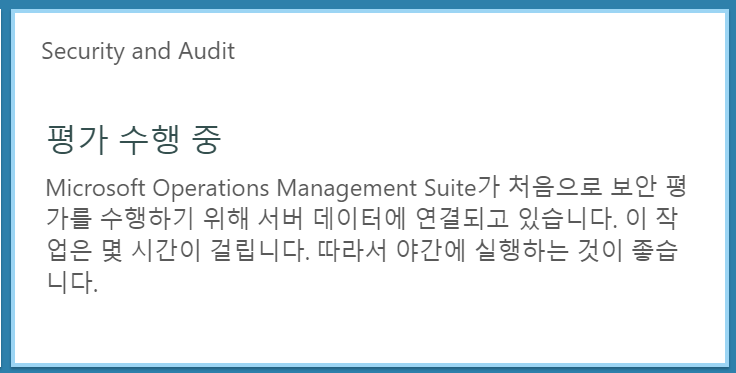
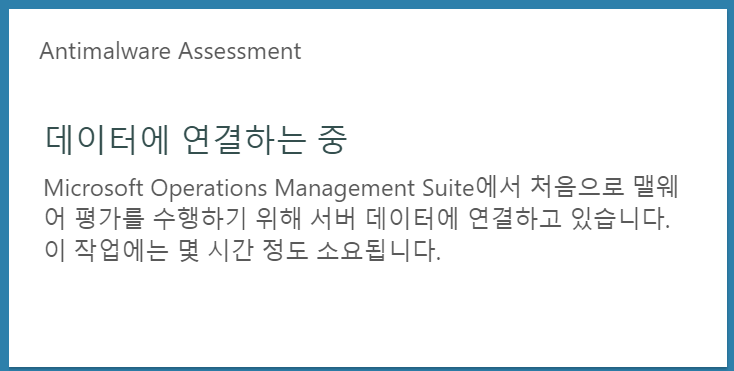
각각의 솔루션을 선택하면 솔루션에 대한 설명과 사용할 서비스 목록이 나타납니다.

“Security & Compliance” 선택



다음과 같은 화면이 나타나고 완료되면 자동으로 서비스가 대시보드에 추가됩니다.

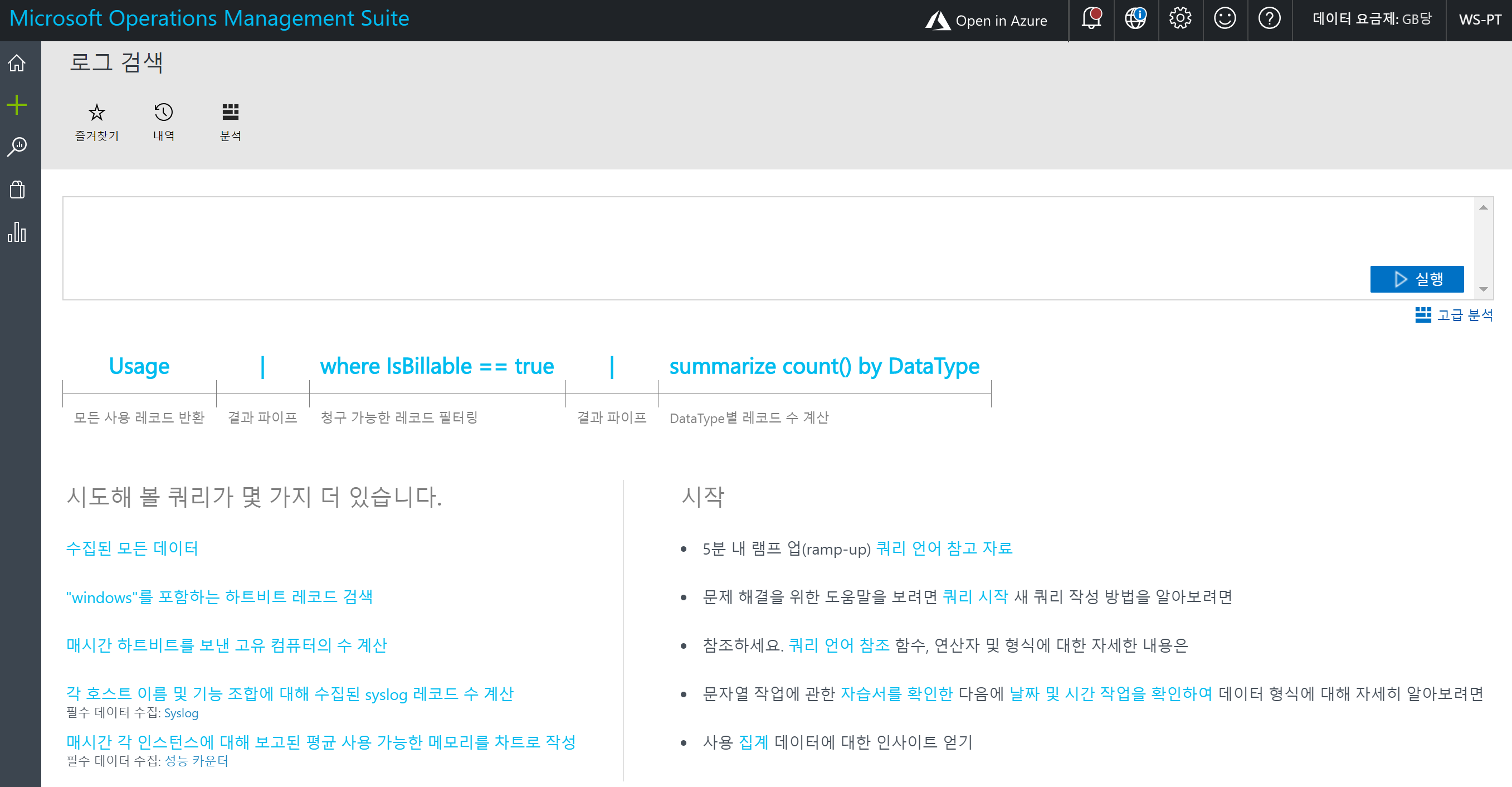




서버 데이터를 연결하는 데에는 시간이 소요됩니다. 따라서 OMS Setting을 진행하실때는 야간에 실행하는 것을 추천드립니다. 해당 부분은 시나리오2에서 실습해볼 수 있습니다.

1. OMS Agent를 통해 저장되는 로그를 쿼리하는 방법에 대해 알아봅니다.

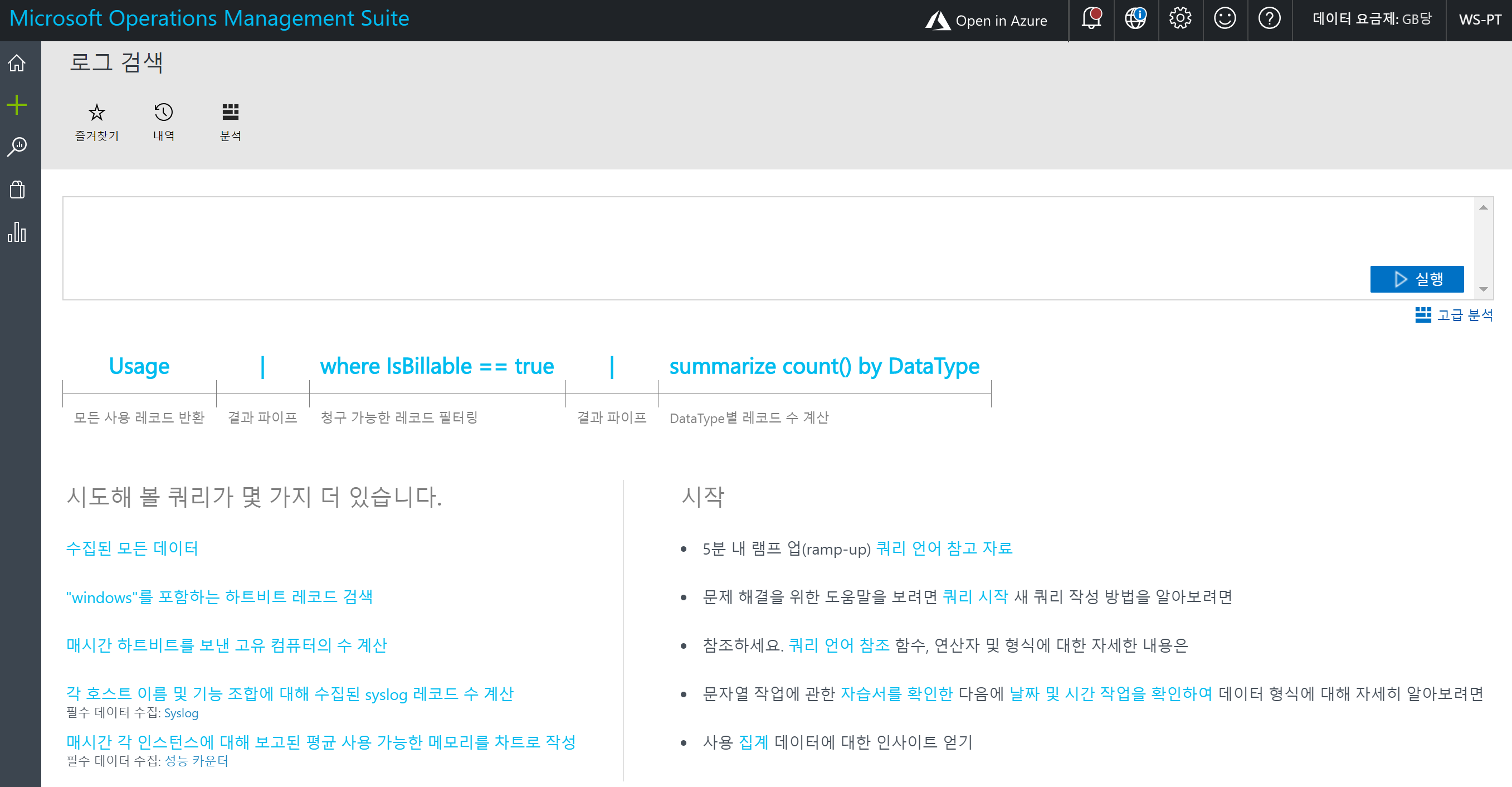
OMS Portal 에 들어가 “로그 검색”을 선택합니다.



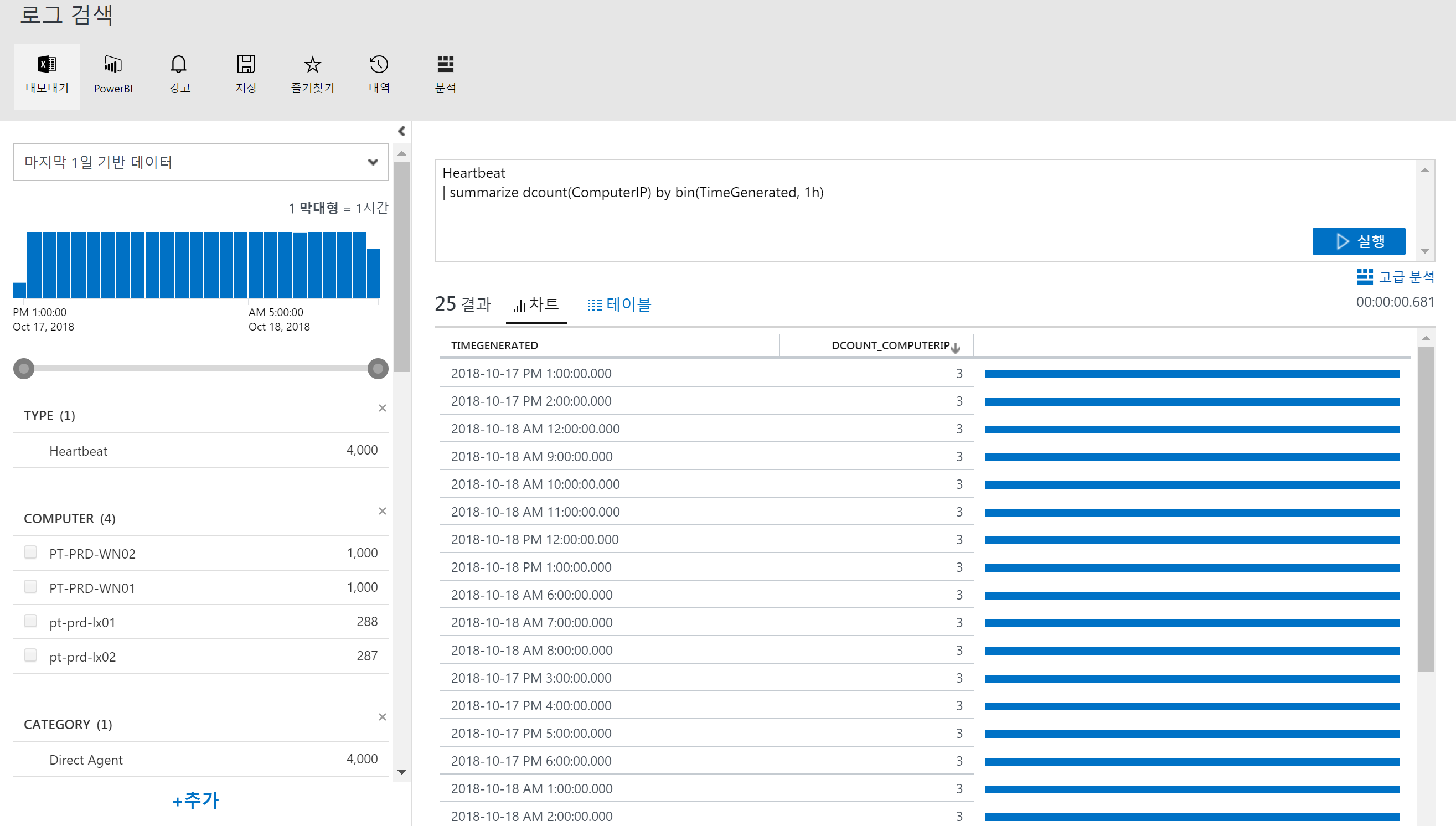
아래에 시도해볼 수 있는 쿼리들이 예시로 나와있습니다.

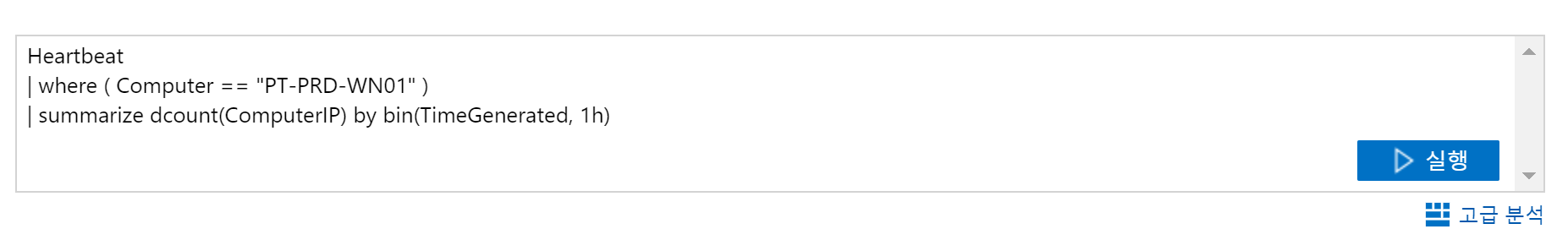
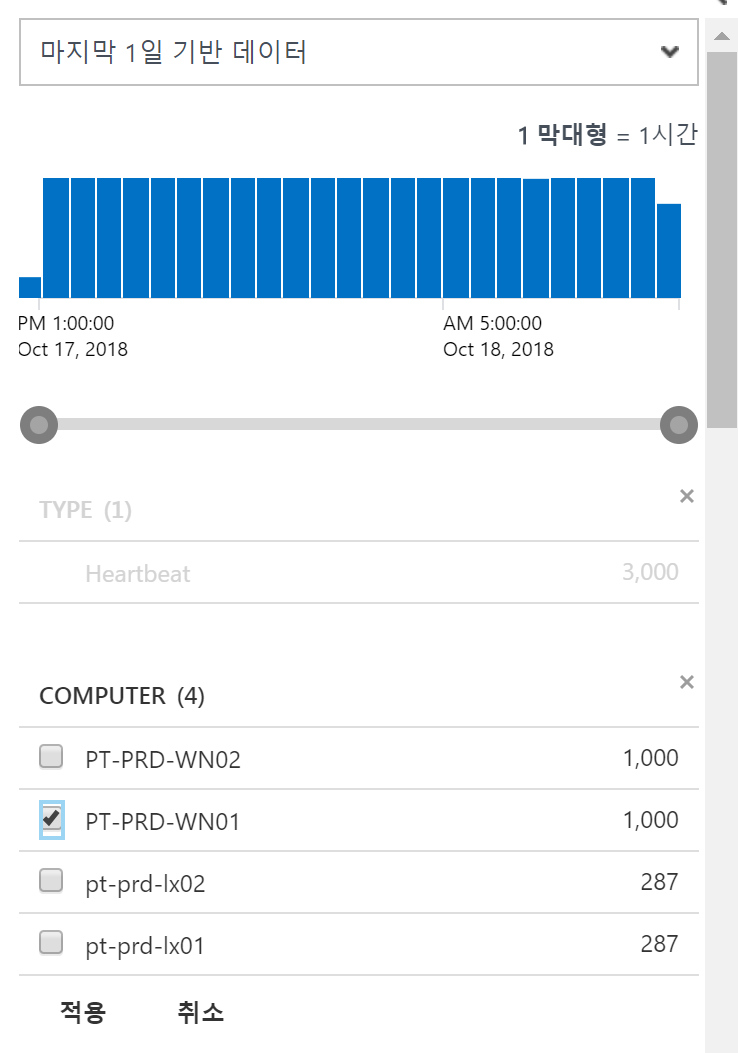
**시나리오1. OMS에 정상적인 하트비트를 보낸 고유 컴퓨터 수 확인**

1. 테스트를 위해 “매시간 하트비트를 보낸 고유 컴퓨터의 수 계산”을 선택합니다.



선택을 하게 되면 기본적인 쿼리와 결과 화면이 나타나게 됩니다.



1. 왼쪽에 있는 항목들을 선택하게 되면 관련 쿼리가 구체적으로 구성되게 됩니다. 

**시나리오 2. 갤러리를 이용한 결과 확인 및 쿼리 확인**

OMS는 솔루션 갤러리를 기반으로 서비스를 사용할 수 있습니다. 현재 Security & Compliance 솔루션이 설치되어 있는 상태입니다. (17-19 page 참고 ) 솔루션이 제공하는 기능과 관련하여 쿼리를 사용하는 방법에 대해 알아봅니다.

1. OMS Portal 대시보드 화면을 보면 Security & Compliance 솔루션이 활성화 된것을 확인할 수 있습니다.

(Security and Audit, Antimalware Assessment)

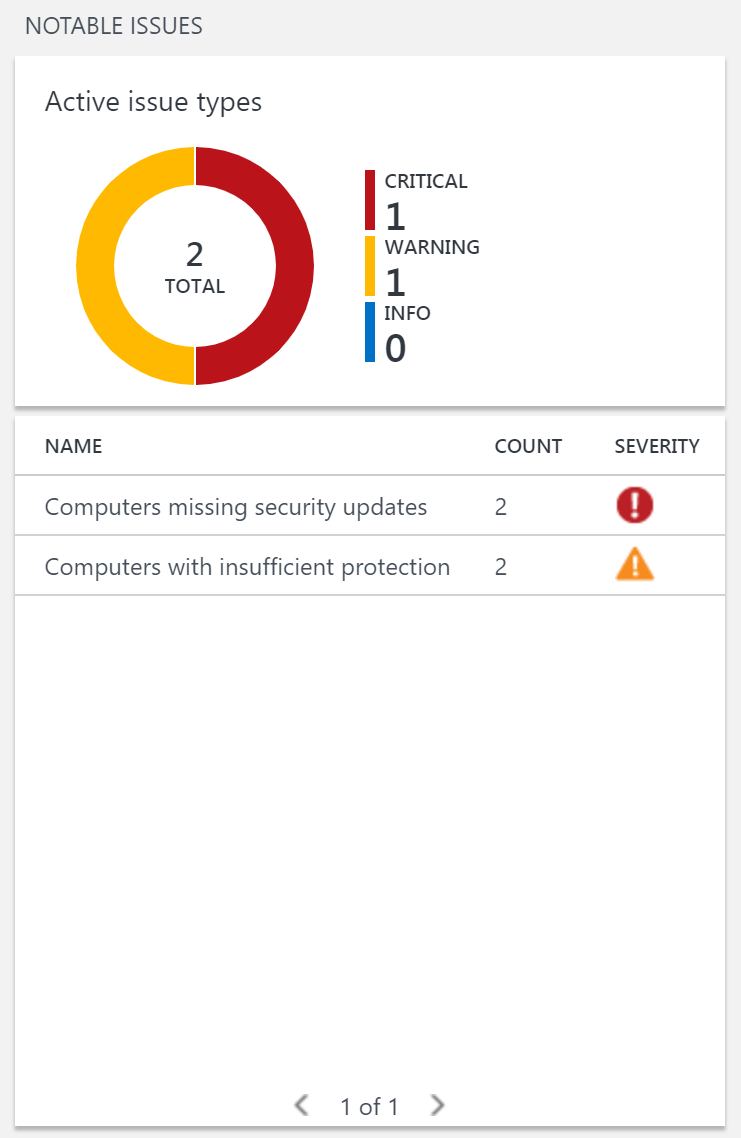
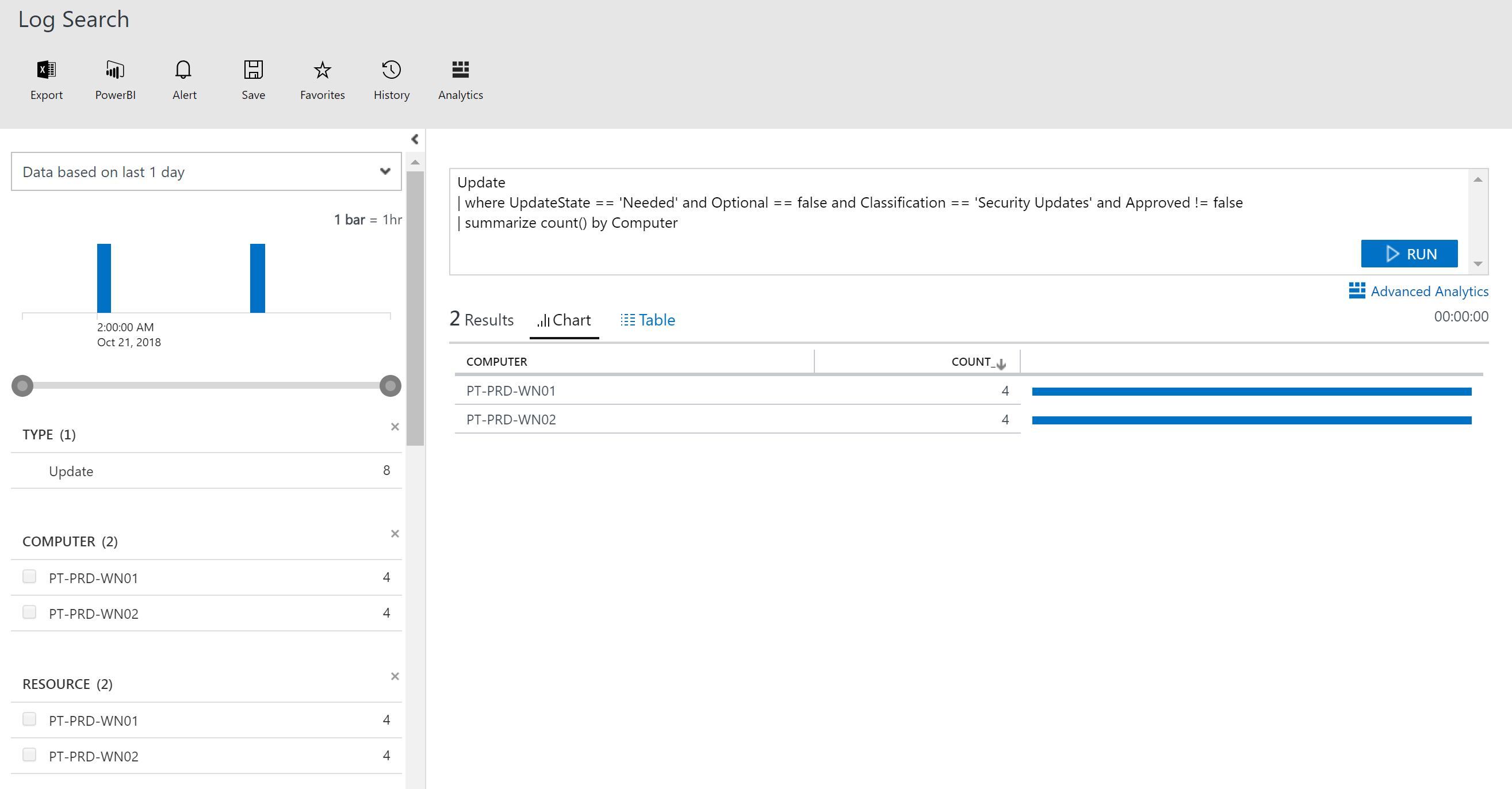


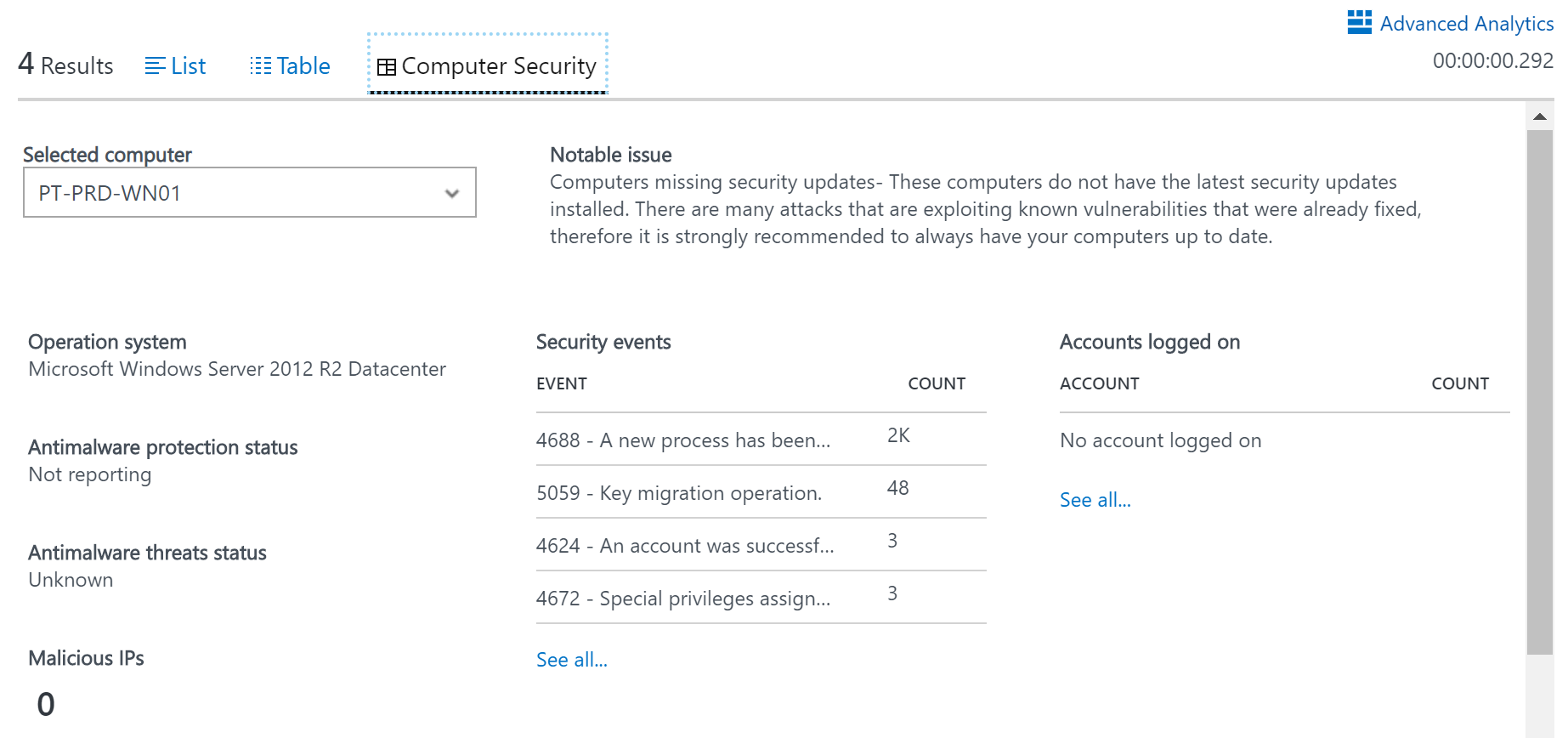
1. Security and Audit을 선택합니다.

보안에 관련하여 전반적인 내용이 대시보드에 나타나고 있으며 선택하면 더 자세한 내용을 볼 수 있습니다.



1. “Notable Issues”에서 “Severity”가 Critical한 항목을 선택해 해당 내용을 확인합니다.



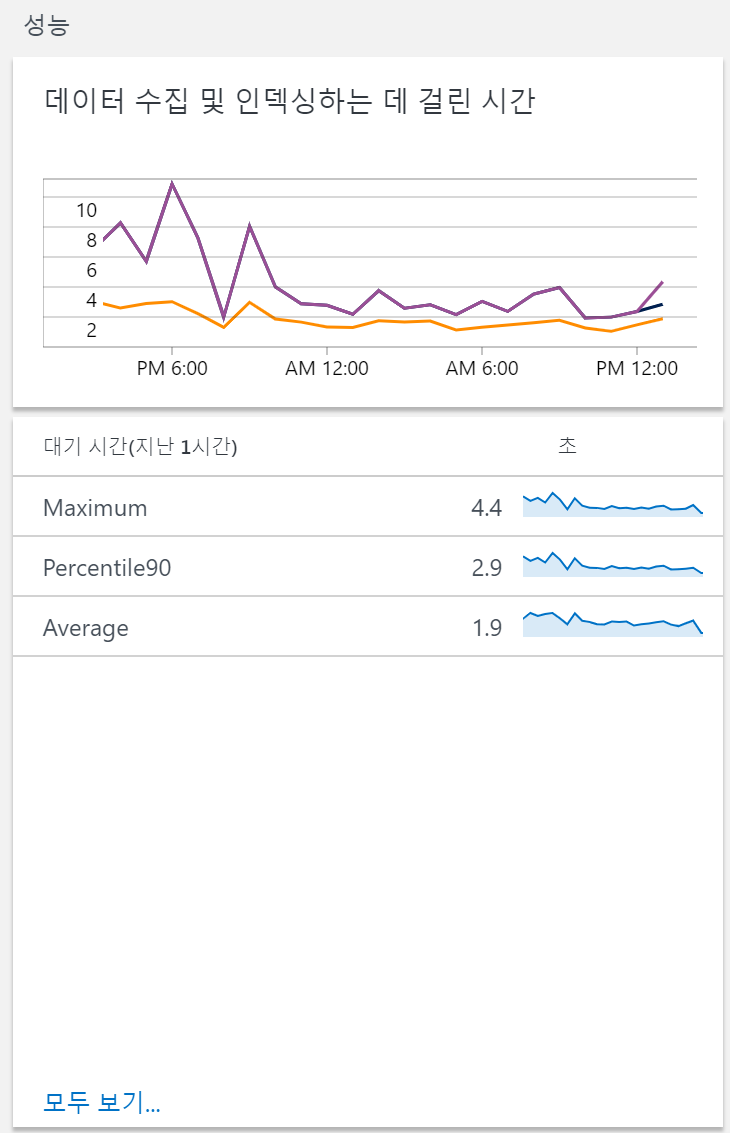
**시나리오 3. OMS 사용량 확인**

OMS는 OMS 사용에 대한 로그를 제공합니다.

“OMS Portal” -> “사용량” 선택



데이터 볼륨, 컴퓨터, 제공, 성능, 쿼리 목록에 대한 사용량을 제공하고 있습니다.



## Lab 3. Azure 보안 센터(Security Center) 사용하기

Azure Security Center는 하이브리드 클라우드 워크로드에 통한 보안 관리 및 고급 위협 방지를 제공하고 있습니다.

보안 센터(Security Center)를 사용하여 워크로드에 대한 보안 정책 적용, 외부 공격에 대한 검색 및 대응이 가능합니다.

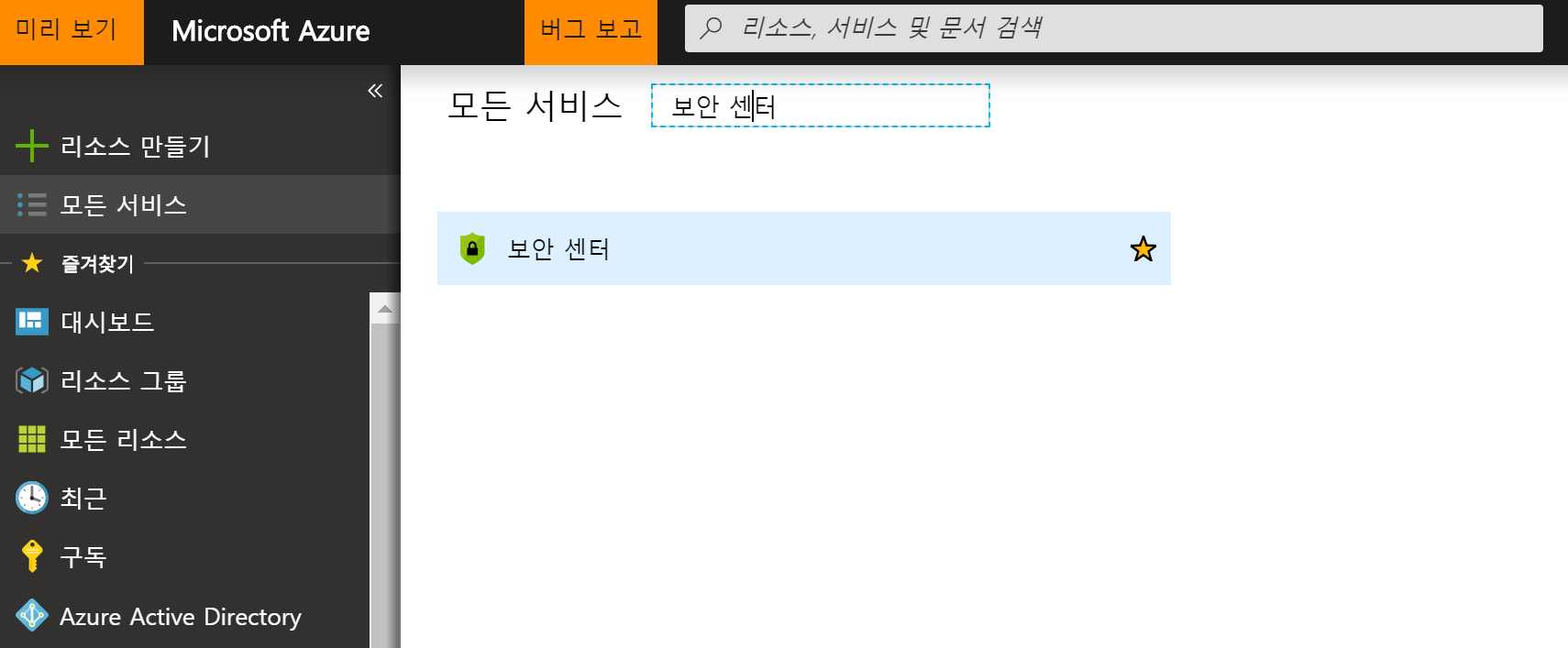
보안센터 특장점

* 중앙 집중식 정책 관리 – 모든 하이브리드 클라우드 작업에 걸쳐 보안 정책을 중앙에서 관리하여 회사 또는 규정 보안 요구 사항을 준수할 수 있습니다.
* 연속 보안 평가 – 가상 머신, 네트워크, 저장소 및 데이터 서비스, 응용 프로그램의 보안 상태를 모니터링하여 잠재적인 보안 문제를 찾아낼 수 있습니다.
* 실행 가능 권장 지침 – 우선 순위가 지정된 보안 권장 지침을 사용하여 공격자들이 악용하기 전에 보안 취약성을 수정할 수 있습니다.
* 경고 및 인시던트 우선 순위 지정 – 우선 순위가 지정된 보안 경고와 인시던트를 통해 가장 중요한 위협부터 중점적으로 확인할 수 있습니다.
* 고급 클라우드 방어 – 관리 포트 및 적응형 응용 프로그램 제어에 대한 Just-In-Time 액세스를 통해 가상머신에서 실행되는 응용 프로그램을 제어함으로써 위협을 줄일 수 있습니다.
* 통합 보안 솔루션 – 연결된 파트너 솔루션을 포함한 여러 소스에서 보안 데이터를 수집, 검색 및 분석할 수 있습니다.

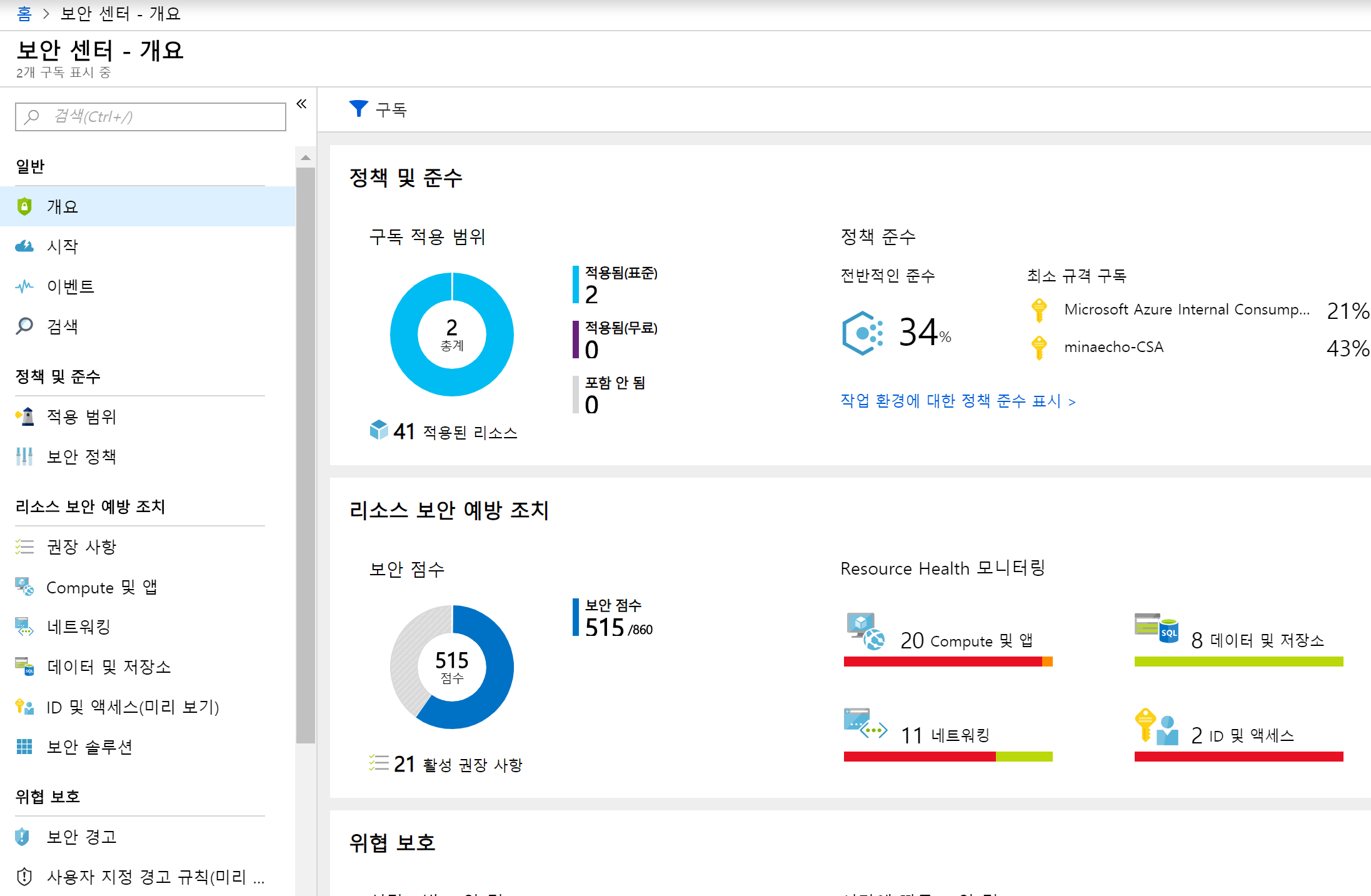


1. Azure 보안 센터 설정하기

Azure Portal에서 “모든 서비스” 선택 후 “보안 센터”를 검색합니다.



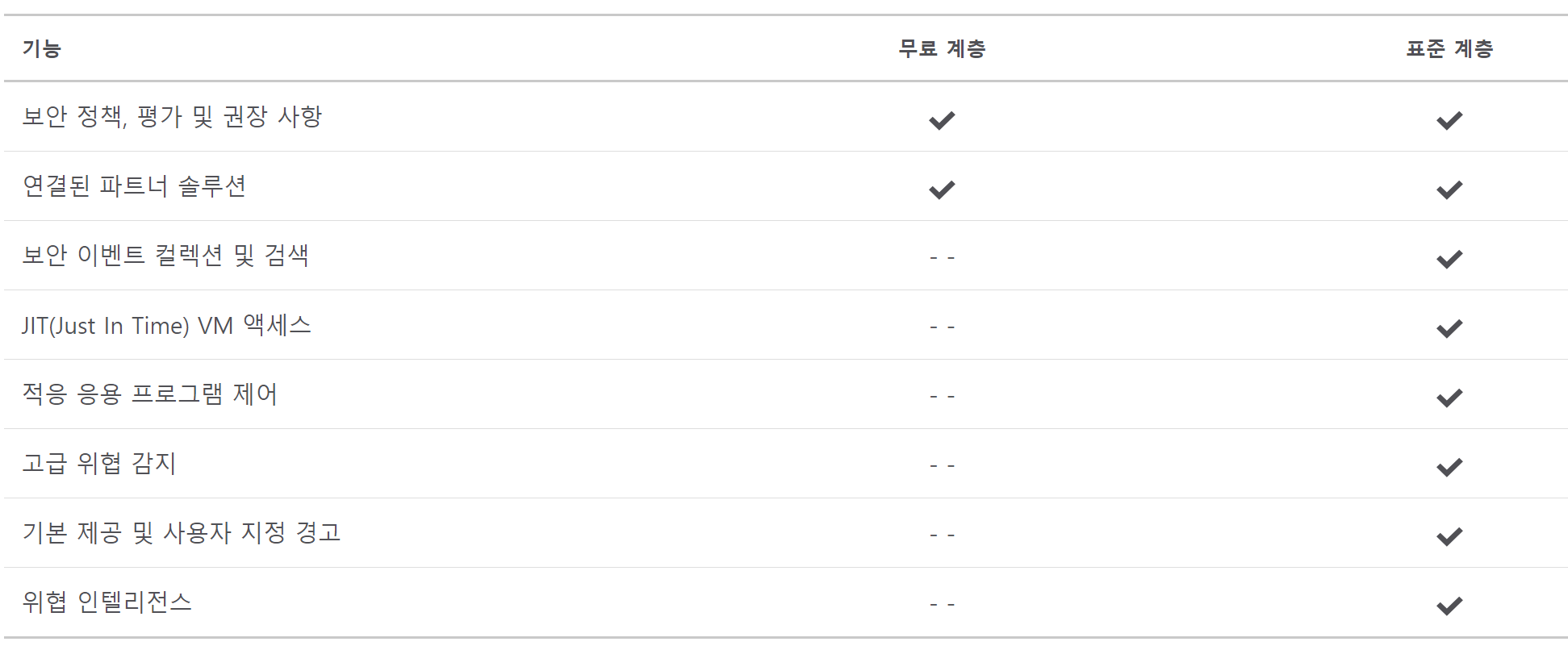
보안 센터의 화면은 다음과 같이 구성되어 있습니다.



보안 센터를 사용하려면 먼저 적용 범위와, 보안 정책을 설정하여야 합니다.

적용 범위는 무료와 표준 계층으로 나뉘어져 잇습니다. 무료와 표준은 지원하는 범위가 조금 다르며 표준 계층의 경우 처음 60일간 무료로 제공됩니다. 60일을 초과하면 사용량 기반으로 요금이 과금됩니다.

금액에 관련된 부분은 해당 url을 참고해주세요.( <https://azure.microsoft.com/ko-kr/pricing/details/security-center/>) 현재 시나리오는 “표준 계층” 을 사용합니다.



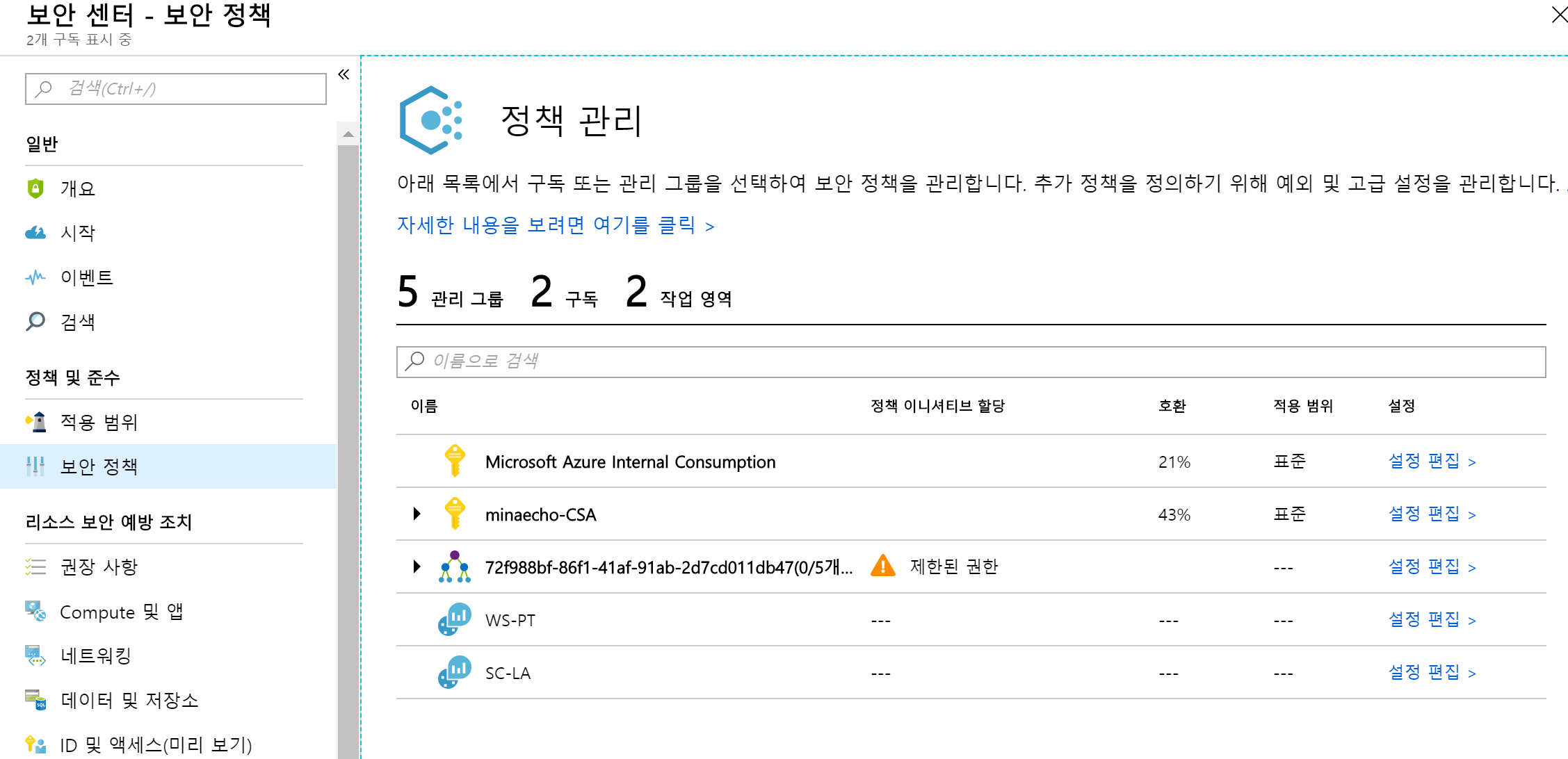
1. 적용 범위, 보안 정책 설정

“정책 및 준수” 에 들어가 구독 또는 관리 그룹에 대한 보안 정책을 관리합니다.

“보안 센터” -> “적용 범위” -> “표준 적용 범위”



“정책 및 준수” -> “보안 정책



“보안 정책” -> “데이터 수집” -> Windows 보안 이벤트

“일반” -> “저장”

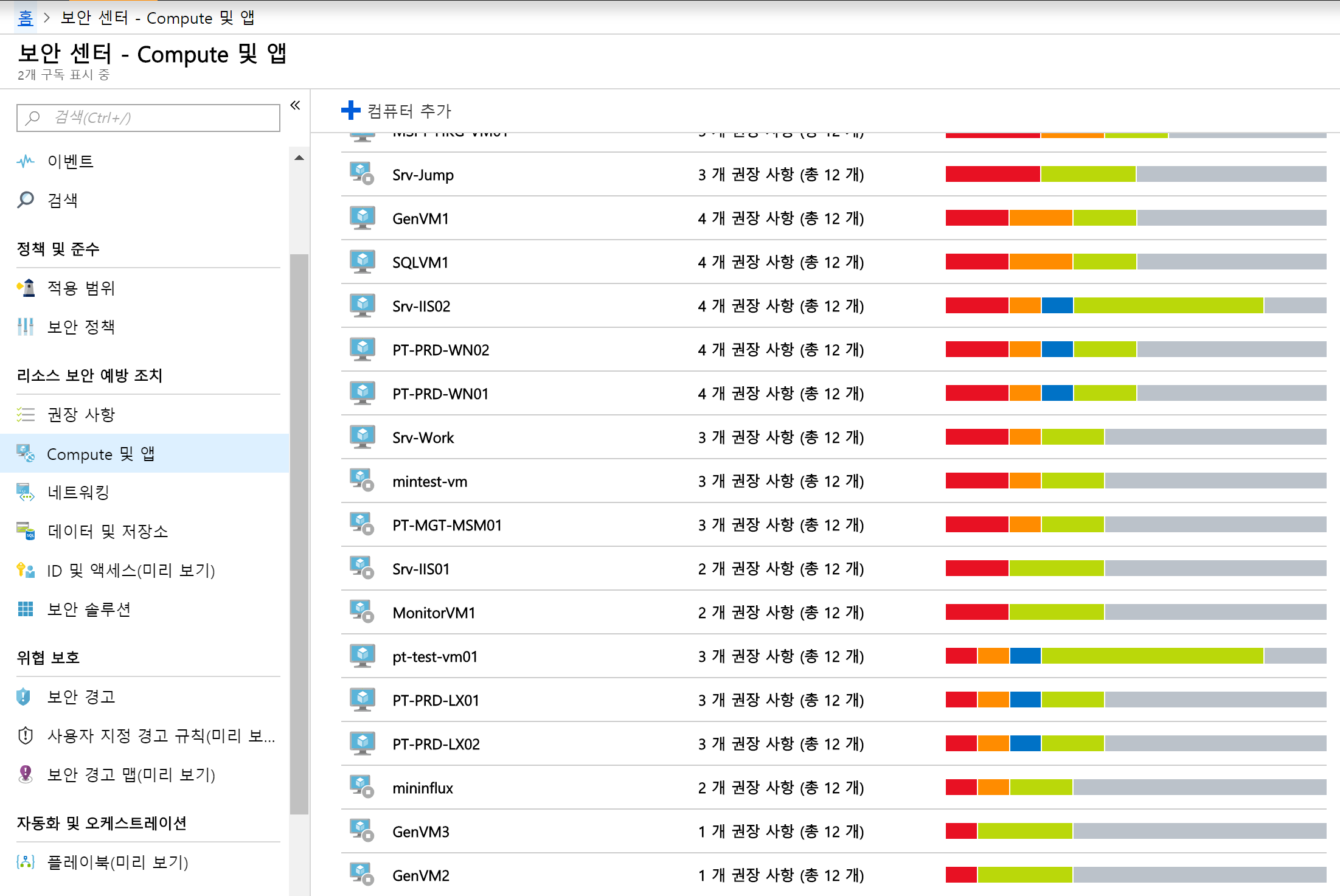


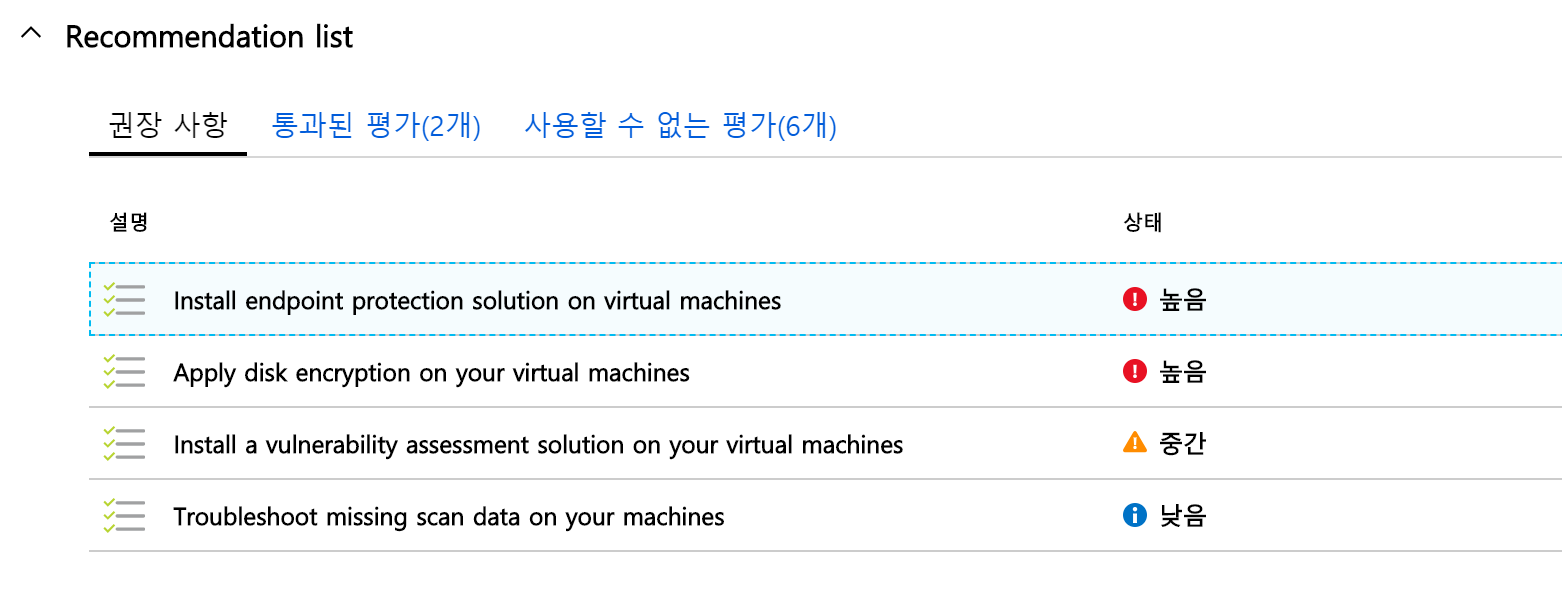
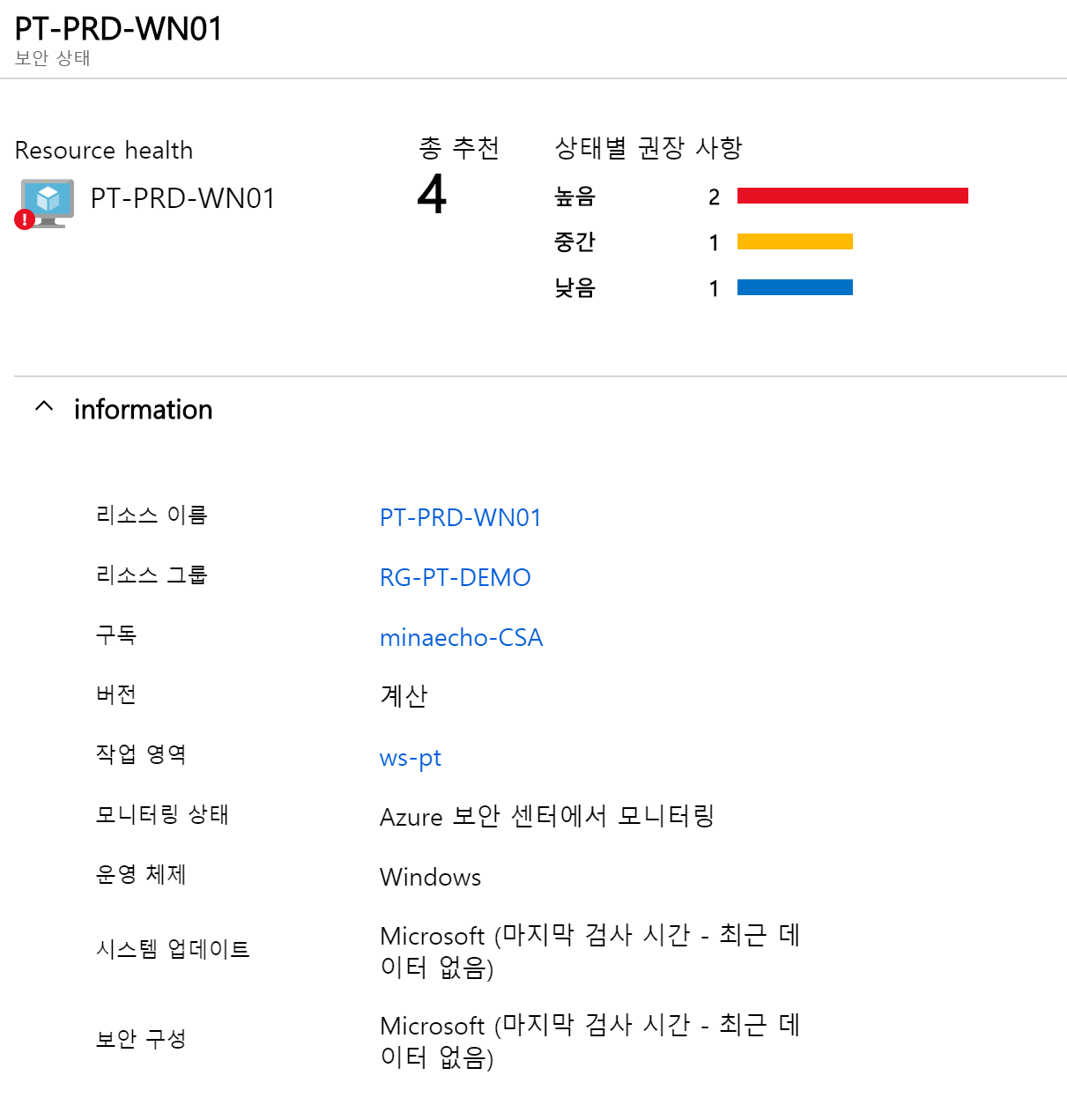
1. Azure Security Center 기능 알아보기

Azure Security Center가 제공하는 기능에 대해 알아봅니다.

**시나리오 1. 리소스 보안 예방 조치**

“보안 센터” -> “리소스 보안 예방 조치” -> “Compute 및 앱” -> 확인할 가상 머신 선택 (“PT-PRD-WN01”)

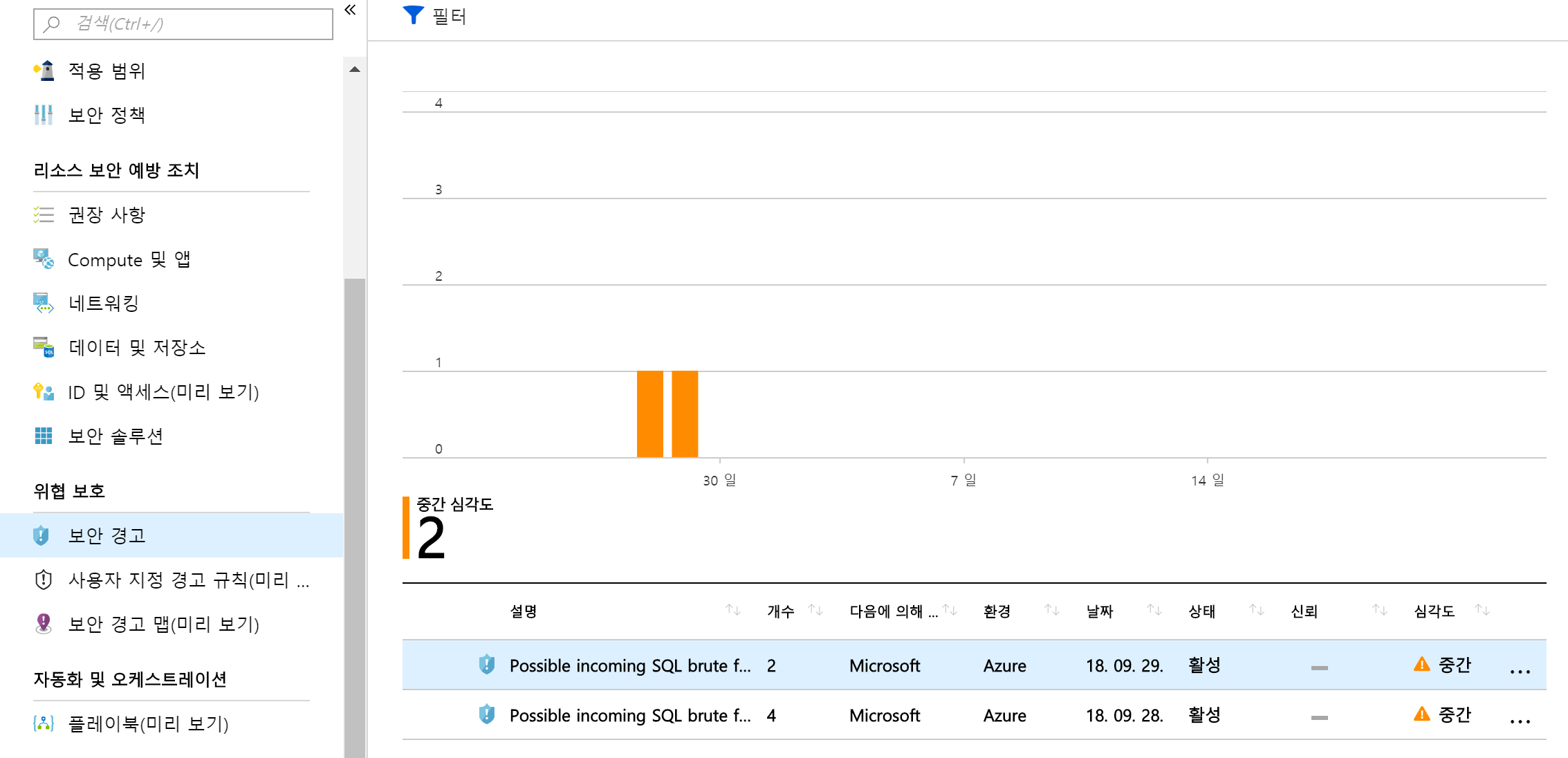




**시나리오2. 위협 보호**

Azure Security Center는 외부에서부터 오는 위협을 감지 및 보호합니다. 또한 기계 학습을 사용하여 패턴을 분석하여 보안에 대한 경고를 줍니다.

**“위협 보호” -> “보안 경고”**



눌러보면 공격 받은 리소스와 관련 상세 정보를 알 수 있습니다.

